**A New Architecture for Network Intrusion Detection and Prevention**

**Abstract:** This paper presents an investigation, involving experiments, which shows that current network intrusion, detection, and prevention systems (NIDPSs) have several shortcomings in detecting or preventing rising unwanted traffic and have several threats in high-speed environments. It shows that the NIDPS performance can be weak in the face of high-speed and high-load malicious traffic in terms of packet drops, outstanding packets without analysis, and failing to detect/prevent unwanted traffic. A novel quality of service (QoS) architecture has been designed to increase the intrusion detection and prevention performance. Our research has proposed and evaluated a solution using a novel QoS configuration in a multi-layer switch to

Organize packets/traffic and parallel techniques to increase the packet processing speed. The new architecture was tested under different traffic speeds, types, and tasks. The experimental results show that the architecture improves the network and security performance which is can cover up to 8 Gb/s with 0 packets dropped. This paper also shows that this number (8 GB/s) can be improved, but it depends on the system capacity which is always limited.

**Index Terms:** Computer security, computer networks, intrusion detection system, intrusion prevention system, network architecture, network security, open source, quality of service, security, and switch configuration.

**Existing system:**

Threats and attacks may range from stealing personal information from a laptop or network server to stealing the most top-secret information stored on a Security Intelligence Service (SIS). Furthermore, hackers can snoop on users' online purchases by eavesdropping on their credit card details, or, even more alarmingly, safety-critical systems can be compromised. Multi-faceted attacks and threats have made the implementation of security systems more challenging. Hackers have evolved along with the sophistication of the IT industry. For example, hackers exploit the developments in computer processors and network speeds to increase the volume and speed of malicious traffic that might constitute the associate editor coordinating the review of this manuscript and approving it for publication was Ali Kashif Bashir. A Denial of Service (DoS) or Distributed Denial of Service (DDoS) attack. Network security is therefore extremely important and has developed into an industry aimed at improving applications and hardware platforms to

Identify and stop network threats.

**Disadvantages:**

One of the most established concepts in information security is a defense-in-depth approach which utilizes a multilayered structural design, in which firewalls, vulnerability assessment tools (anti-viruses and worms), and IDPS (Intrusion Detection and Prevention Systems) are employed to prevent any hostile endeavors on network systems and servers.

**Proposed system:**

One of the most established concepts in information security is a defense-in-depth approach which utilizes a multilayered structural design, in which firewalls, vulnerability assessment tools (anti-viruses and worms), and IDPS (Intrusion Detection and Prevention Systems) are employed to prevent any hostile endeavors on network systems and servers. The Network Intrusion Detection and Prevention System

(NIDPS) has been designed to serve as the last point of defense in the network architecture. NIDPS monitor the transportation of network traffic for any malicious and uncomfortable activities and create alerts when operating in detection mode or block packet alerts when operating in prevention node . The detection and prevention mechanisms of the NIDPS are grounded in observing the comparison of ingress packets (traffic) to any known attack through patterns (signature NIDPS mechanism) or identifying unknown malicious patterns from ingress traffic (anomaly NIDPS mechanism).

**Advantages**

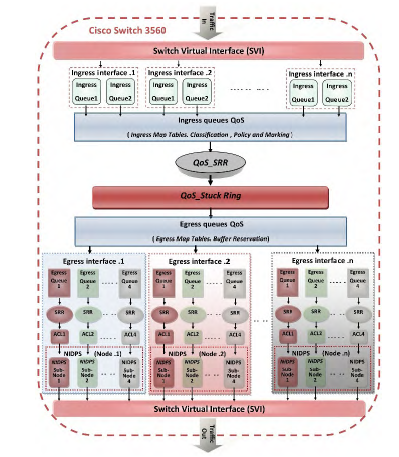
1. Counter intrusions or malicious attempts to access networks and systems.

2. Analyze network traffic and identify hackers' targets and techniques; and detect or prevent unwanted and malicious traffic.

3. The research investigates how QoS including DiffServ technology and parallelism can have impact in high-speed and heavy traffic networks using an industry standard switch and standard desktop processors.

4.This solution is a more accessible way of receiving good results as it can be activated at a higher level, namely at the level of configuring the switch software and replicating Short on standard machines. Further improvements could be made if higher performance equipment was used. Cost is generally an important concern. The design proposed in this research benefits the network security requirements at low cost.

**Architecture:**



**Modules:**

**QoS Classification And Policy Methods:**

Classification is the process of identifying the data packets to a class or group in order to manage the packet appropriately. QoS features such as a policy map and class map can be used to achieve this. The class information can be assigned by switch, router, or end host. Policing involves creating a policy that defines a group weight (the number of bytes to be processed together) for the traffic and applies it to the interface. Policing can be applied to a packet per direction and can occur on the ingress and egress interfaces. Different types of traffic can be recognized in terms of type, and ports and differentiated policies can be set accordingly

**Parallel Technology with QoS:**

Parallel NIDPS is a form of computation where many NIDPS nodes work simultaneously, operating on the principle that the large incoming data can be divided into smaller sets, which are processed at the same time. Parallelism of NIDPS can occur at three general levels: the high-level processing node (entire system), the component level (specific tasks are isolated and parallelized) and the sub-component level parallelism (function within a specific task)

**QoS Classification, Policing And Marking For Ingress And Egress Interfaces (Queues):** Queues, class, and policy technologies can use access control lists (ACLs) to allow the processing management of different types and patterns of incoming and outgoing packets. The novel configuration proposed in this paper uses an ACL technology with a class map and SVI

Queues, as well as a policy map that specifies each type of IP traffic (e.g., ICMP, TCP and UDP) to be processed by implementing parallel output queues with associated parallel NIDPS nodes

**Conclusion:**

A new architecture for NIDPS deployment was designed, implemented and evaluated. There has recently been massive development in computer networks regarding their ability to handle different speeds and data volumes. As a result of this rapid development, computer networks are now more vulnerable than ever to high-speed attacks and threats. These can cause considerable trouble to computer networks and systems. Network intrusions can be categorized at various levels. Many high-speed attacks can be classified as being difficult to detect or prevent. It will become ever more difficult to analyze increasing volumes of traffic due to the rapid shifts in technology that are increasing network speed.

**Software Requirements**

Operating System : Windows XP/2003 or Linux (Any OS)

User Interface : HTML, CSS

Client-side Scripting : JavaScript

Programming Language : Java

Web Applications : JDBC, Servlets, JSP

IDE/Workbench : My Eclipse 8.6

Database : Oracle 11g

Server Deployment : Tomcat 7.0

**Hardware Requirements (Minimum)**

Processor : Intel core i3 or above

Hard Disk : 500GB or more

RAM : 8GB or more

**Future work:**

Statistical based anomaly detection is designed to detect deviations from a baseline model of network behavior. When the rate of ``malicious'' packet transmission is very high, the attack will almost certainly be detected by a statistical anomaly detector.