EXPLORATIONS ON ENGINEERING LETTERS (EEL)
VOLUME 1, ISSUE 1 (2016):PP.61-67
SANA ACADEMIC PRESS

Robust Deep Packet Inspection Traffic Classification

Ramya Mythily. U[1], S.Gowri[2], S.Brindha[3]
[1]Research Scholar, [2,3]Assistant Professor,
Dept. of Computer Science & Applications,
St.Peter's University, Chennai, India
ramyamythili89@gmail.com

Abstract-*Classification of traffic is only the first step that helps identify different applications and Various actions, such as monitoring, rechecking, discovery, control, and optimization can then be performed on the identified traffic with the goal of improving the network performance. Deep Packet Inspection is a form of computer network packet filtering that examines the data spam, intrusions, or defined criteria to decide whether the packet may pass or if it needs to be redirected to a different destination, or, for the purpose of collecting statistical information. There are multiple ways to obtain packets for deep packet inspection. Using port mirroring(sometimes called Span Port) is a very common way and then an optical splitter.Deep Packet Inspection (and filtering) enables advanced network management, user service, and security functions as well as internet data mining, eavesdropping, and internet censorship.*

Keywords: *Datapackets,DPI,collision*

I. Introduction

Robust deep packet inspection is used to control the network traffic by inspecting the data packet to handle the errors. Here each and every data packet is handled and the errors or collision which occurred is cleared and then redirected to the destination location. If the destination address is lost while transmitting the data packets, the data packet is again sent back to the source to resend the data packets again to the destination. If any errors or collision occurs then the errors are handled first and then it will be sent to the destination. If collision occurs in the data frame then the data is discarded and then error free data from the buffer is reset in to the data packet. This procedure is done to each and every data packets which have been sent from the source to the destination. This technique is achieved by using the data flow inspection algorithm. Which treat the errors at the beginning stage of the data transmission, so that the collision is controlled during the data transfer phase. After checking the data packet for any errors and collision, then the data packets are transmitted through the network. Which finds the optimized path for the data to be transmitted which minimum hops. At the last stage once the data packets have been successfully transmitted to the destination node an alert is sent back to the source for the confirmation that data packets have been successfully sent. This approach is efficient and reduces the error, collision and data loss.

Drawbacks

Concurrently the existing traffic classification suffers from poor performance when the zero day traffic are present due to misclassification of zero day traffic into predefined known classes. Traffic still exist in network due to data packet.

What is DPI ?

Using DPI, communications service providers can allocate available resources to streamline traffic flow. For example, a message tagged as high priority can be routed to its destination ahead of less important or low-priority messages the security implications of DPI are widespread because the technology makes it possible to identify the originator or recipient of content.

Packets

Most networks transmit data in small blocks called packets which helps to detect transmission errorsGives fair access for a shared connection between many computersThese are packet networks or packet switching

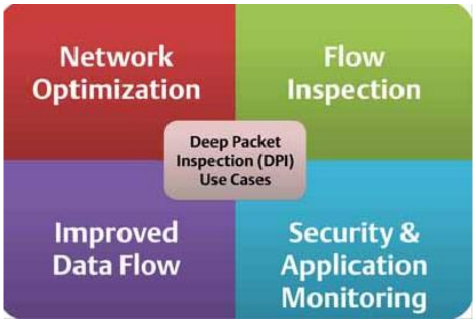
DPI limitations

DPI has at least three significant limitations. First, it can create new abilities as well as protect against existing problems like collision and conflict. Second, DPI adds to the complexity and unwieldy nature of existing firewalls and other security-related software like anti virus and antispyware. Third, DPI can reduce computer speed because it increases the burden

II.Literature survey

Deep packet inspection in residential gateways and routers: Issues and challenges
MP-DPI: A network processing platform based on the many-core

Deep packet inspection


Network Optimization
Flow Inspection
Deep Packet Inspection (DPI) Use Cases
Improved Data Flow
Security & Application Monitoring

Deep packet inspection or DPI is now a fast growing application technology in the field of network security, which requires the network security platform has a higher speed to handle a large number of session connections, and track the status of these connections quickly. This paper proposed the MP-DPI, a many-core based network processing platform, which uses the ATCA standard modular design, makes use of the integrated many-core network process accelerate engine, and integrates a popular open source DPI system named SNORT. The experiment result shows that in the same power consumption, the throughput of MP-DPI platform is three times as large as traditional X86 servers.

Network Optimization: This serves the purpose of optimizing the traffic which happens due to overload and collision.

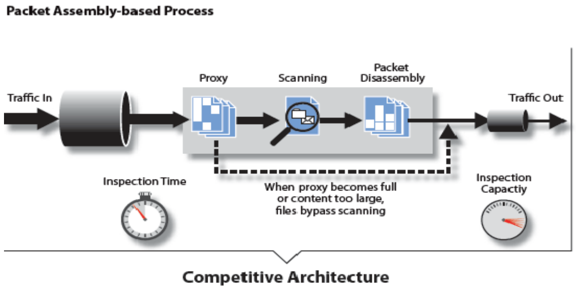
Flow Inspection: This inspects the flow of data packets which have been sent to the network to prevent overload and collision.

Improved Dataflow: This check for a shortest path to make the dataflow between source and destination efficient.

Security and Application Monitoring:

Security of dataflow is checked in each and every level to prevent loss /theft of data. Application monitoring helps to monitor the dataflow in and every stage.

Architecture



The above architecture shows how the data packet with traffic or collision is treated. Data packet with traffic is sent to be scanned, once the packets are scanned the data packets are disassembled. Then the data packets without any errors are again re-transmitted to the network. Inspection time is set for the data packets to detect and correct the data packets. Inspection capacity is also set to avoid data overflow in the packet inspection process.

Network optimization

Network Optimization is an important component in the effective management of information systems. As information technology is growing at an exponential rate, this continued growth adds to the strain of already over-stressed network architecture within an organization. Shortest Path Problems, The Max-Flow Problem, The Min-Cost Flow Problem, Simplex Methods for Min-Cost Flow, Nonlinear Network Optimization, Auction Algorithms for Min-Cost Flow and Dual Ascent Methods for Min-Cost Flow

Error Detection and Correction

First we need to detect errors. First step in error detection and correction is to detect errors. This is achieved by checking the error bit. The bit when set to 1 mean, that error is present in the data which is sent through the network. Sender includes some extra (redundant) information that summarizes the original data. Buffer frame include the redundant information of the original data. In case of collision or data loss the redundant information can be utilized. Receiver checks this Receiver checks for the accuracy of the data. Various schemes, differing in various severe complexity, data overhead and robustness Then we need to decide what to do, Error correction or Retransmission

II. FLOW INSPECTION- SNIFFER ANALYSIS

Pinpoint performance issues and isolate the root cause, so you can rapidly rectify and solve network performance problems before they become create any problems for users.

The need for granular insights into the application and network performance

Regardless of the complexity of any organization’s applications and networks, operations teams are expected to keep everything perfect and running under any circumstances. In order to accomplish this, you need granular-level insights to check the performance so you can quickly troubleshoot problems.

Overcoming Problems in all Complex Environments

An inability to effectively troubleshoot complex applications and networks can leave your operations at risk. NetScout’s Sniffer Analysis helps you to get the source of the problem quickly by conducting granular, packet-level analysis the target performance issues and identifies root causes.

Unprecedented granular packet forensic analysis capabilities

NetScout’s Sniffer Analysis provides unprecedented granular packet forensic analysis capabilities that change and simplify troubleshooting. This makes innovative product to perform granular packet analysis, mining and decoding of packets captured and stored by InfiniStream appliances. As a result, you can quickly pinpoint performance anomalies and immediately isolate the root cause, allowing you to rapidly solve the most challenging problems.

Sniffer Analysis helps for the following:

Conduct packet-level analysis , Quickly pinpoint performance anomalies .Isolate root causes so that network operations staff can easily solve complex application and network performance issues.

Data Flow Performance

To configure the Data Flow task for better performance, you can configure the task's properties, adjust buffer size, and configure the package for parallel execution. Adjust the Sizing of Buffers. Configure the package for parallel. Configuring individual data flow components. Avoid unnecessary sorting.

Network security

Network security consists of the rules, policies and methods adopted to prevent and monitor unauthorized access, misuse, modification, or access denial of a computer network and network-accessible resources. Network security involves the authorization of access to resource in a network, which is controlled by the network administrator.

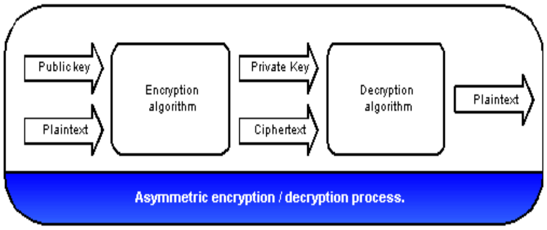
Many network security threats today are spread over the Internet. The most common include: Viruses, worms, and Trojan horses, Spyware and adware, Zero-day attacks, also called zero-hour attacks, Hacker attacks, Denial of service attacks, Data interception and theft and dentity theft.

How Network Security Work?

Network security is accomplished through hardware and software. The network security software need be constantly updated and managed to protect from emerging threats. A network security system usually consists of many components. Ideally, altogether all components work together, which minimizes maintenance and improves security. Network security components often include, Anti-virus and anti-spyware, Anti-virus- is a software designed to detect and destroy computer viruses. Anti-spyware – is a software type of program designed to prevent and detect unwanted **(spyware)** program installations and to remove those programs if installed .Intrusion prevention systems (IPS),is a system to identify fast-spreading threats, such as zero-day or zero-hour attacks. Firewall, to block unauthorized access to your network. Virtual Private Networks (VPNs), is to provide secure remote access

Security process

Security is an important aspect in data transmission. Security ensures that data is prevented from unauthorized access. Data are secured using encryption and decryption algorithm. Encrypted data are sent to the network to be transmitted and at the receiving end the data is decrypted and utilized. Encryption and decryption is achieved using private key and cipher text. Private key is a secure key which is available only within the source and destination. Using this private key the data frame in the data packet will be encrypted and the data in the data packet is decrypted using the same private key.



Data Packet Inspection-Algorithm

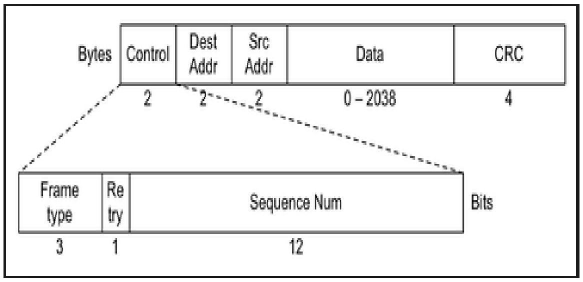
```
while  pckCnt > 0:
for i in validate[pckCnt ]:
if (pckCnt[i].Err ==True):
{
  if(pckCnt[i].Priority=='High'):
    {
       if(pckCnt[i].ErrType=='Collision'):
        {
              new DataPack;
             //  set packet Priority ='High'
               Priority='High';
```

```
                DA=destination address;
                SA=Source address;
            // discard Collision data;
                 Del Data;
           // Replace the collision data with new data
    Data= new collision free data;
      }
      else if(pckCnt[i].ErrType=='Loss of DA'):
        {
             Redirect to SA;
        }
  pckCnt -1
```

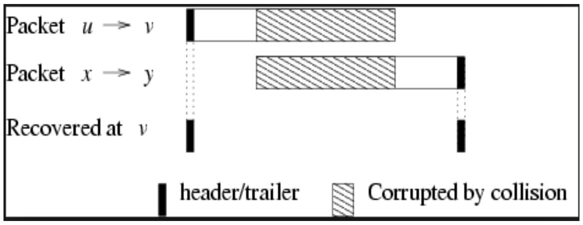
Step1: Checks the count of the data packets. **Step2:** If the data packets count is greater than zero, the checking process starts or else comes out of the loop. **Step 3:** It checks the Err bit to see whether the error bit is ‘True’ or ‘False’. If the Err bit is ‘True’, the error correction process is applied or else comes out of the loop. **Step 4:** Then the ‘Priority’ of the error is checked. If the priority is ‘HIGH’ then the ‘ErrType’ is checked. **Step 5:** If ‘ErrType’ is ‘Collision’ then , collapsed data is replaced with the original data from the buffer. **Step 6: If ‘**ErrType’ is 'Loss of DA' then, the data packet is sent back to the source address. **Step 7:** This procedure is done for each and every data packets in the network.

DataFlow Approaches

There are two approaches to perform network analysis for information flows.
Static approach- to check the conformity of the formally described physically and logical connections between network . Dynamic approach- to check the real data flow detected in the network flows for conformity to the policy flow model. Data flow in the network can be done using the following, Hub, Switches, Translational switching, Fat pipes, Broadcast throttling, Fragment-free switching, Spanning tree protocol for loop resolution, Virtual LANs (VLANs) and Routers. The following technologies enable routers to perform specialized functions to improve information flow and establish a "first defense" against network intruders: Traffic filtering and firewalling, Traffic prioritization, Traffic grouping, Variety of routing and routed protocols supported. Two types of routing protocols are commonly used they are Distance Vector Routing Protocols and Link State Routing Protocols. Over years the network traffic occurs during transmission of data over network. This is currently rectified by checking the collision of data packets and then resolving it further minimizes the network traffic.



The figure describes the architecture of the data packets. It has five sections the first is the control ,second the destination address of the data packet ,third the source address of the data packet, fourth the data section and fifth the CRC cyclic redundancy check to avoid redundancy in the data section.



The above figure shows the data packets which have been corrupted and recovered at the specific point during transmission.

IV . Conclusion

Robust deep packet inspection allows data packets to be transmitted in the network without any errors and collisions. But, need each and every packet which is sent to be inspected before passing it towards the destination. This leads to performance, but in turn need lot of time for inspection. This scheme is not efficient for large amount of data packets. And this requires two phase of analysis on to detect errors and another for efficient optimized data flow. As the number of data packets increases the performance of the inspection algorithm comes down.

REFERENCES

[1]. Cisco Systems, Inc., San Jose, CA, USA, “Cisco WAN and application optimization solution guide,” Tech. Rep., 2008 [Online]. Available: http://www.cisco.com/c/en/us/td/docs/nsite/enterprise/wan/ wan_optimization/wan_opt_sg.html

[2]. T. Nguyen and G. Armitage, “A survey of techniques for Internet traffic classification using machine learning,” *IEEE Commun. Surveys Tuts.,*vol. 10, no. 4, pp. 56–76, 4th Quart., 2008.

[3]. H. Kim *et al.*, “Internet traffic classification demystified: myths, caveats, and the best practices,” in *Proc. ACM CoNEXT Conf.*, 2008, pp. 1–12.

[4]. J. Zhang *et al.*, “Network traffic classification using correlation information,”*IEEE Trans. Parallel Distrib. Syst.*, vol. 24, no. 1, pp.104–117, Jan. 2013.

[5]. A. Tongaonkar, R. Keralapura, and A. Nucci, “Challenges in networkapplication identification,” in *Proc. 5th USENIX Conf. Large-Scale ExploitsEmergent Threats*, 2012, pp. 1–3.

[6]. A. Moore and D. Zuev, “Internet traffic classification using Bayesiananalysis techniques,” *Perform. Eval. Rev.*, vol. 33, no. 1, pp. 50–60,2005.

[7]. T. Auld, A. Moore, and S. Gull, “Bayesian neural networks for Internet traffic classification,” *IEEE Trans. Neural Netw.*, vol. 18, no. 1, pp.223–239, Jan. 2007.

[8]. A. Este, F. Gringoli, and L. Salgarelli, “Support vector machinesfor TCP traffic classification,” *Comput. Netw.*, vol. 53, no. 14, pp.2476–2490, 2009.