IDPSE: A Network Intrusion and Prevention System with Edge Computing

1st Chengjun Jia
Tsinghua University
Beijing, China
jcj18@mails.tsinghua.edu.cn

2nd Yunpeng Luo
Tsinghua University
Beijing, China

3rd Yifan Li

***Abstract*—IDPSE (Network Intrusion Detection Prevention System with Edge Computing)[1]**
***Index Terms*—DDoS**

I. Introduction

Challenges: 1. IPv4 + NAT, IPv6 is not common. It is hard to block a specific IP. 2. DDoS is still annoying: We can detect it easily but we can hardly guarantee the QoS especially when the network is congested. 3.

In summary, this paper makes the following contributions:

- As far as we know, the paper is the first paper focusing on the infrastructure of implementing IDPS from the aspect of Cloud and Edge Computing().
- With the help of Edge Computing, IDPS can prevent the
- Convert the placement of Network Security Service into an optimization problem.
- Based on some industry data which we collected and measured, we demonstrate that Edge Computing will not increase xxxx and on which condition, IDPS can
- Compared with all service placed in Cloud or placed in Edge, we calculate the decrease of cost and others, to demonstrate the advantages of our System. We make some simulations/experiments to measure the overload of.

When we put them together, it is surprising that Edge Computing can help build a more 'secure' network, encouraging us to consider about how to implement some Network Security Service under the environment of Edge Computing.

[1]Network Intrusion Detection and Prevention System, as NIDPS, IDPS or IPS. In the paper, IDPS refers to Network Intrusion Detection and Prevention System. We also have the other IDPS, called Host IDPS.

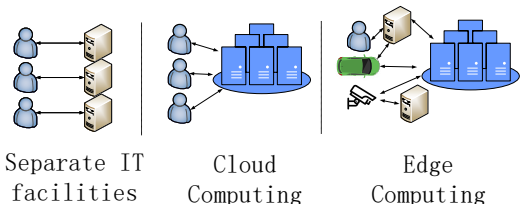

Fig. 1: IT Infrastructure Development

II. Background and Motivation

In the section, we give a brief overview of Edge Computing (EC) and introduces some EC applications which work better than those without EC. It encourages us to think about how to make full use of EC to provide better service in Computer Network. We choose IDPS as a perspective, reviewing the development and some challenges of IDPS. It is surprising that EC indeed gives us some important opportunities for IDPS.

A. Edge Computing: A new IT infrastructure

Information Technology (IT) infrastructure combines physical components and various software to provide an organization with the ability to focus on the documents and programs without caring about the maintenance of IT facility. [3] Physical components include some computing, storage and networking hardware while software components include Operating System and some important Application software such as Nagios and Puppet, which are required to deliver, control, test or monitor IT services.

The development of IT Infrastructure is depicted in Fig-1. Traditionally, enterprises deploy its own IT facilities and they are separate physically. With the development of Cloud Computing from 2005 [2], more and more companies tend to deploy IT infrastructure within a public, private or hybrid cloud computing system, in which the resource utilization ratio can be higher for an organization and the capacity is flexible for an user. However, with more and more data generated at the edge and growing quantity of devices connected to the network,the network bandwidth and latency is becoming the bottleneck. A new computing paradigm, edge computing, appears. Edge Computing allows for computation performed at the edge of network, reducing the response latency and energy consumption compared with Cloud Computing.

Mobile Edge Computing (MEC) is notable in EC because the share of wireless traffic in Computer Network is growing nowadays. In 5G wireless systems, specialized communication hardware is replaced by generic servers with Network Function Virtualization (NFV). As a result, small-cell base stations have some extra computation capacity to play the role of Edge Server, bringing us more optimization space to take full advantage of IT resources.

Although Cloud Computing is still the mainstream at present, EC has attracted some researchers and many companies. Many Cloud Computing enterprises, CDN enterprises or Internet Service Providers are investing on it, such as AWS, Fastly and AT&T Labs. VideoEdge [1] balances the resource usage and the accuracy of video analytics queries under the circumstance of EC. EC also helps the efficiency of Caching, improving the QoS for users [4]. These examples show us the development potential of EC.

B. Challenges of IDPS

IDPS can prevent and monitor misuse or denial of IT resources, by evaluating suspected intrusions, which are overlooked by firewall, and stopping it once it has taken place. IDPS is very important in Network Security and can resist both passive and active attacks, such as Port scanner, Denail-of-Service, Buffer overflow and SQL injection.

Although IDPS has appeared since 1986, there are still some challenges now. The first and most important challenge is the problem about update. Because of the emerging network attacks, IDPS usually needs to update itself on time. Enterprises need to pay for not only the IDPS but also the newest databases or algorithms in it.

The second challenge is the scalability of IDPS. A large signature database would be necessary for IDPS if the Security Department has no clear idea of what IT service will be deployed. Rules for both Windows OS and Linux OS, for both SQL and Oracle, are deployed in IDPS, making the process flow complicate and reducing the throughput.

Distributed Denial-of-Service(DDoS) defense is another big problem for IDPS. We need 2k-5k VMs to handle a 100Gbps attack for just **one type** of attack[2], which means that the cost of hardware is about $32k, while 300Gbps defense charges at least $64k every year in industry.

C. New opportunities

Similar as IT infrastructure, IDPS was always implemented with specialized hardware, provided by Cisco or Juniper. The enterprises, as clients, can acquire some IDPS service from Cloud Computing providers thanks to the appearance of SDN and NFV. These facts inspire us to consider about how to implement IDPS under the circumstance of EC.

It is obvious that we need IDPS service at the Edge to provide security for Edge Computing instance. The IDPS at the Edge do not need many rules because the number of IT service is pretty small there. As a result, we may achieve high throughput. Besides, we can implement IDPS and IT service at the same time at the Edge with NFV technology, thus there is no update problem of IDPS. EC instance is very near to the end-hosts and the feature is the solution to reducing the harm of DDoS attack.

[2]There are many different types of DDoS attack, such as DNS Amplification, SYN Flooding and UDP flood

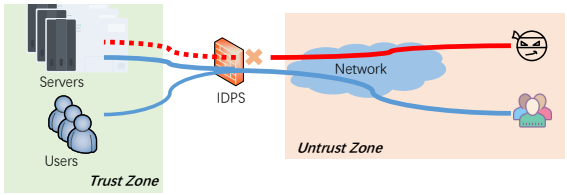

Fig. 2: The Location of IDPS

EC seems to be a good solution to IDPS implementation and we need to look into whether it is correct and how to make full use of the EC features in IDPS implementation.

III. Problem Formulation

In this section, we analyze how IDPS works and then figure out what the challenges are when we want to implement it in the scenario of EC.

A. IDPS

A typical IDPS is placed at a strategic point or points to monitor all traffic between the trust Zone and the untrust Zone, as shown in Fig-2. There are three main components in IDPS: *Monitor*, *Analyzer* and *Actuator*.

- *Monitor* collects the information of network flows. It can be placed on the path or by the path.
- *Analyzer* decides whether a flow is harmful from the information from *Monitor*.
- *Actuator* makes some essential actions on packets of a flow, such as drop the packet or modify some flag bits of packets, to defend the security of IT resources in trust Zone.

In terms of *Analyzer* method, there are two main categories of methods: signatured-based and anomaly-based. The common algorithms in Signatured-based method are String Match, Regular Expression, Access List and so on; the common algorithms in Anomaly-based method are Threshold, Machine Learning, etc.

- In Signatured-based method, some rules are predefined and if a flow matches with any rule, it is judged as harmful.
- In Anomaly-based method, we have some 'innocent' patterns and if any pattern of a flow does not match, we suspect its security.

Although an integrated path in IDPS is from packets to *Monitor* to *Analyzer* to *Actuator*, we can ignore the process of *Analyzer* in Signature-based method because it is quite simple, depicted in Fig-3.

If a flow is classified as 'harmful' by IDPS, it has a tag of *Positive*, otherwise, *Negative*. If a flow is 'malicious' in fact, it has a tag of *Malicious*, otherwise, *Normal*. As a result, the

	Postive	***Negative***
Malicious	True Postive (TP)	False Negative (FN)
Normal	False Postive (FP)	True Negative (TN)

TABLE I: Different kinds of flows through IDPS

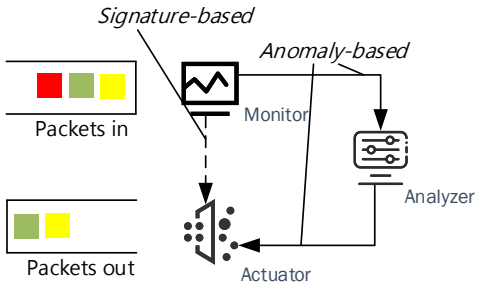

Fig. 3: The Architecture of IDPS

flow through IDPS can be classified as four categories, shown in Table-I and we can define some metrics to compare the performance of IDPS, such as False Positive Rate (FPR) and False Negative Rate (FNR), by counting the number of flows of different categories.

$$FPR = \frac{FP}{FP+TN} \quad FNR = \frac{TN}{FN+TP}$$
$$Precision = \frac{TP}{TP+FN} \quad Accuracy = \frac{TP+TN}{All} \tag{1}$$

Low FPR means that almost all the 'positive' flows are malicious, in the other words, the IDPS with low FPR seldom mistake a normal flow as 'positive' and stop it. Meanwhile, low FNR means that the IDPS usually would not let a malicious flow go even if it 'kills' some innocent. It is common that we can hardly design an IDPS with low FPR and low FNR.

We make a summary of the comparison between signature-based and anomaly-based methods, shown in Table-II; and engineers tend to design a practical IDPS in a hybrid way to combine advantages of the two methods.

	Signature-Based	***Anomaly-Based***
FPR	Low	High
FNR	High	Low
Precision	Low[1]	High
Resource Consumption	Low	High
Rules	Manual	Automatic

TABLE II: The performance comparison of Signature-based and Anomaly-based methods

B. Edge Computing Features and Challenges

There are two distinct features in EC, low-latency to end-hosts and limited compute resources at the Edge. The former can help us prevent DDoS which will show in Sec-?, but the latter is a big problem.

We can view Edge Computing as an extend Cloud Computing. KubeEdge: we need Serveless.

When we think about how to implement IDPS into the Edge Computing.

Flexible: we must allow both the Signature-based and Anomaly-based methods.(ŁŁ)

Efficient: the limited resources at the Edge.

First, there are two parts we need to defend. Because the service between is flexible. We may need to make the resources flexible.

Second, the resources in Edge Computing is small.

Third, the latency between Edge Servers and Cloud Servers is not negligible.

Now that we focus on the infrastructure of IDPS in Edge Computing instead of some detection algorithms, we ignore the algorithms of Analyzer such as DNN, Decision Tree...

IV. System Overview

Based on the analysis above, we envision the deployment model and workflow of IDPSE, outlining our key ideas to address the challenges.

A. IDPSE Infrastructure and workflow

To solve the problem of limited resources at the Edge, we introduce the Cloud resources to offload some works to Cloud. As shown in Fig-4, there are two parts in IDPSE: Edge IPS and Cloud IPS, which collaborate to implement both the Signature-based and Anomaly-based methods. Edge IPS is placed at the point where all traffic go through to the Edge Service while Cloud IPS at the point between Cloud Servers and Internet.

We have four categories of IDPSE workflows with different defend methods and different objects to protect:

- SE: Signature-based method for Edge Service
- SC: Signature-based method for Cloud Service
- AE: Anomaly-based method for Edge Service
- AC: Anomaly-based method for Cloud Service

SE and SC are placed at the Edge while
We decide to place SE and SC at the Edge, AE and AC

B. Placement of workflow

Why do four workflows of IDPSE work as above? Ł
Some obversation or assumptions:

C. Advantages

We could make full use of the advantages of Signature-Based method and Anomaly-Based Method.

V. Implementation & Evaluation

The monitor or detection has three different types:

a) Packet level:

b) Flow level: ACL(Access Control List)

[1]The low precision of Signature-Based method means that it can hardly detect the malicious flows outside the defined rules, while the Anomaly-Based can.

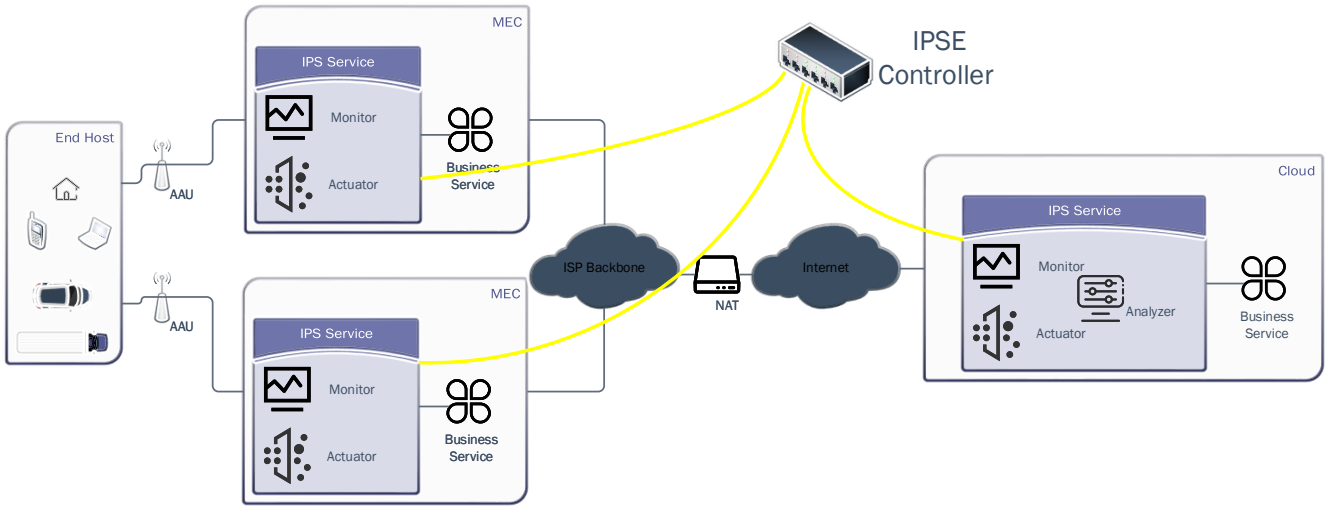

Fig. 4: The Infrastructure of IDPSE

c) Network level: With Go language, we make a simulation about the system.

Compared to the whole IDS system?

TODO: Try to find the benchmark? Similar with a job runned in Spark?

NetFlow(Cisco)

Nowadays, the main problem in Network Security is DDoS and the main algorithms are

VI. Related Work

Bohatei

A. Network Monitor System

sFlow/ Cisco's netflow

such as **Sonata** and **Confluo**.

VII. Conclusions

VIII. Acknowledgement

References

[1] Hung, Chien-Chun, et al. "Videoedge: Processing camera streams using hierarchical clusters." 2018 IEEE/ACM Symposium on Edge Computing (SEC). IEEE, 2018.

[2] JoSEP, Anthony D., et al. "A view of cloud computing." Communications of the ACM 53.4 (2010).

[3] Simon, E. "Distributed Information SystemsFrom Client." Server to Distributed Multimedia, London (1996).

[4] Liu, Dong, et al. "Caching at the wireless edge: design aspects, challenges, and future directions." IEEE Communications Magazine 54.9 (2016): 22-28.