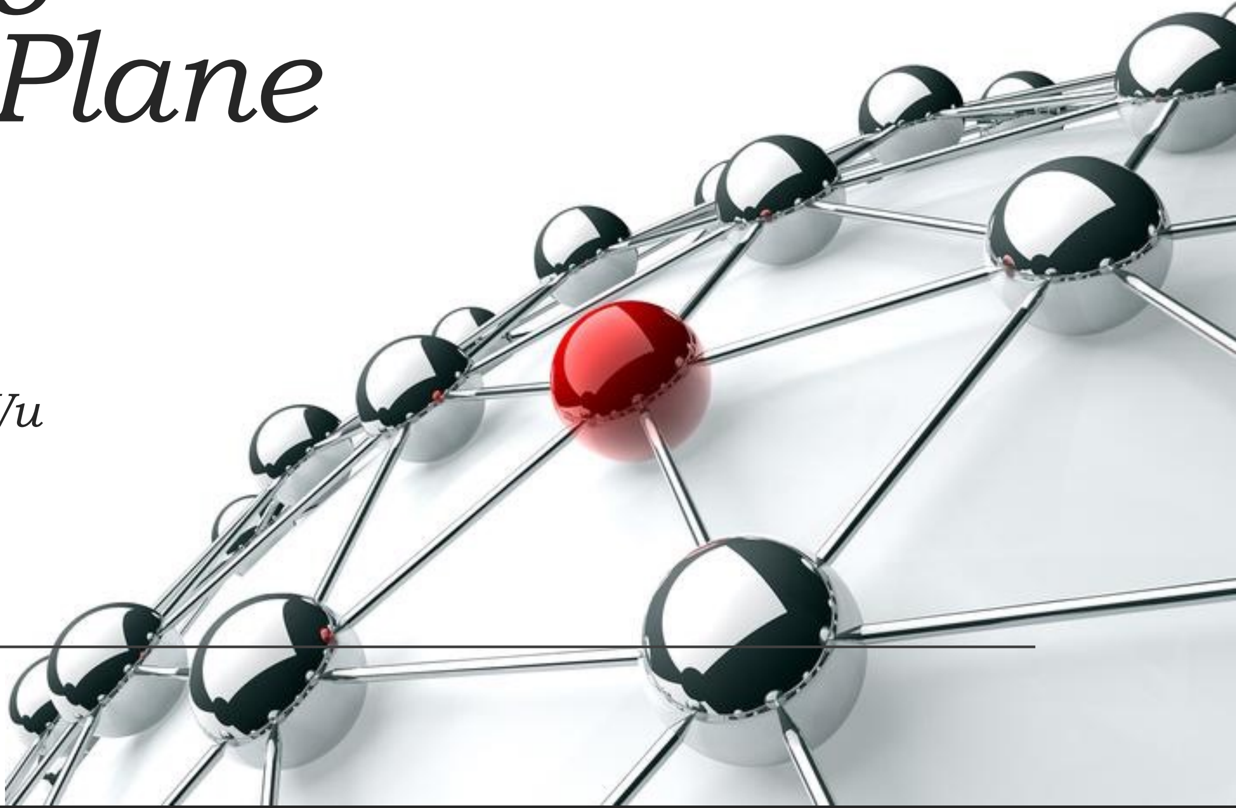
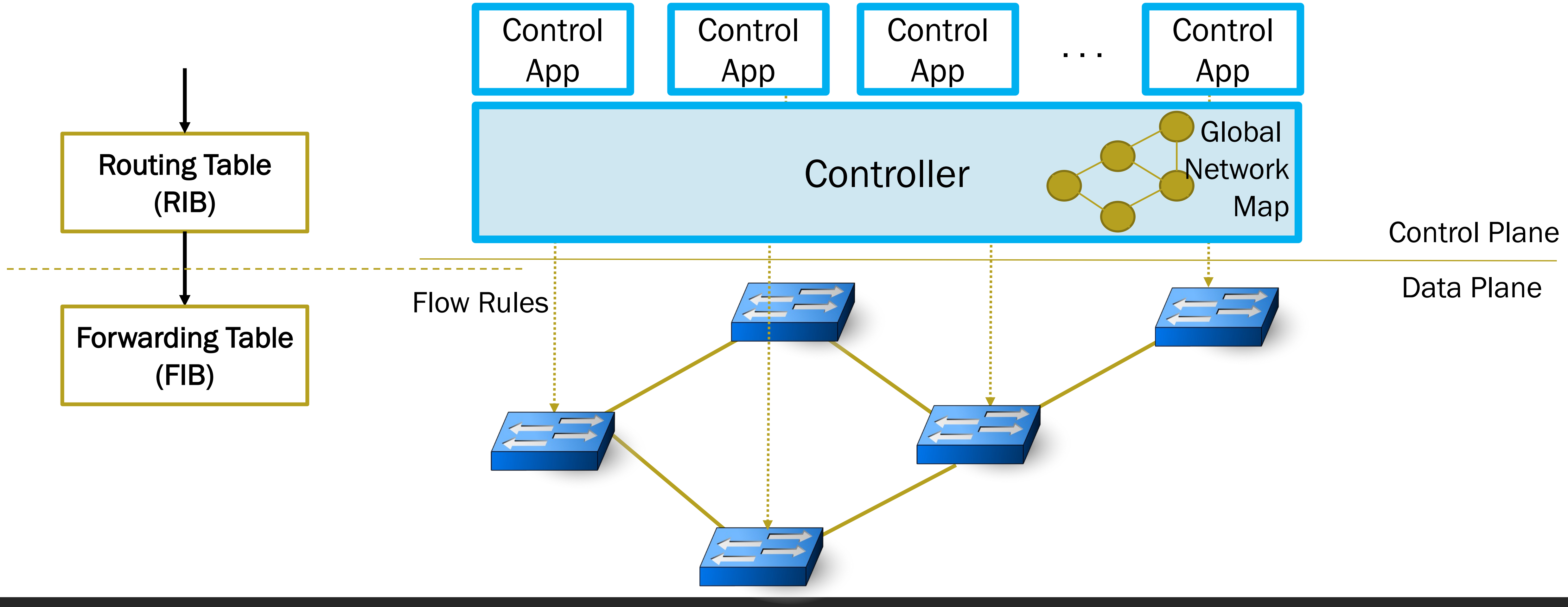
Enhancing Load Balancing by Intrusion Detection System Chain on SDN Data Plane

Nadia Niknami and Jie Wu

Temple University

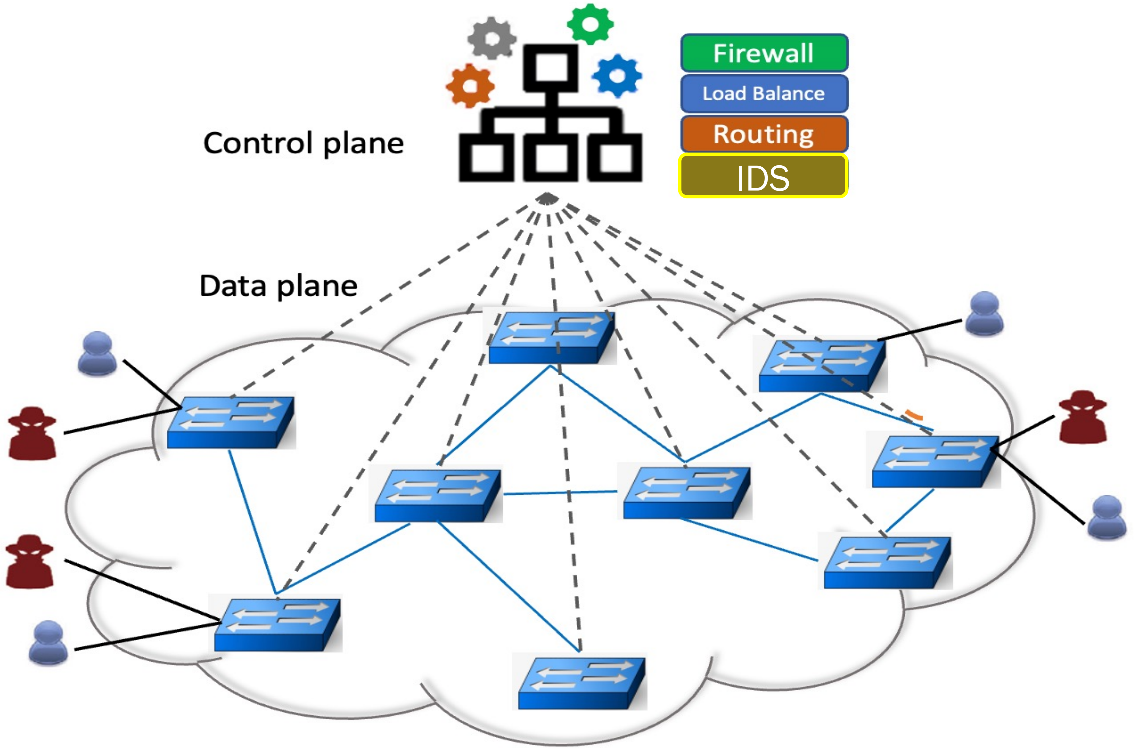


Software-Defined Networks



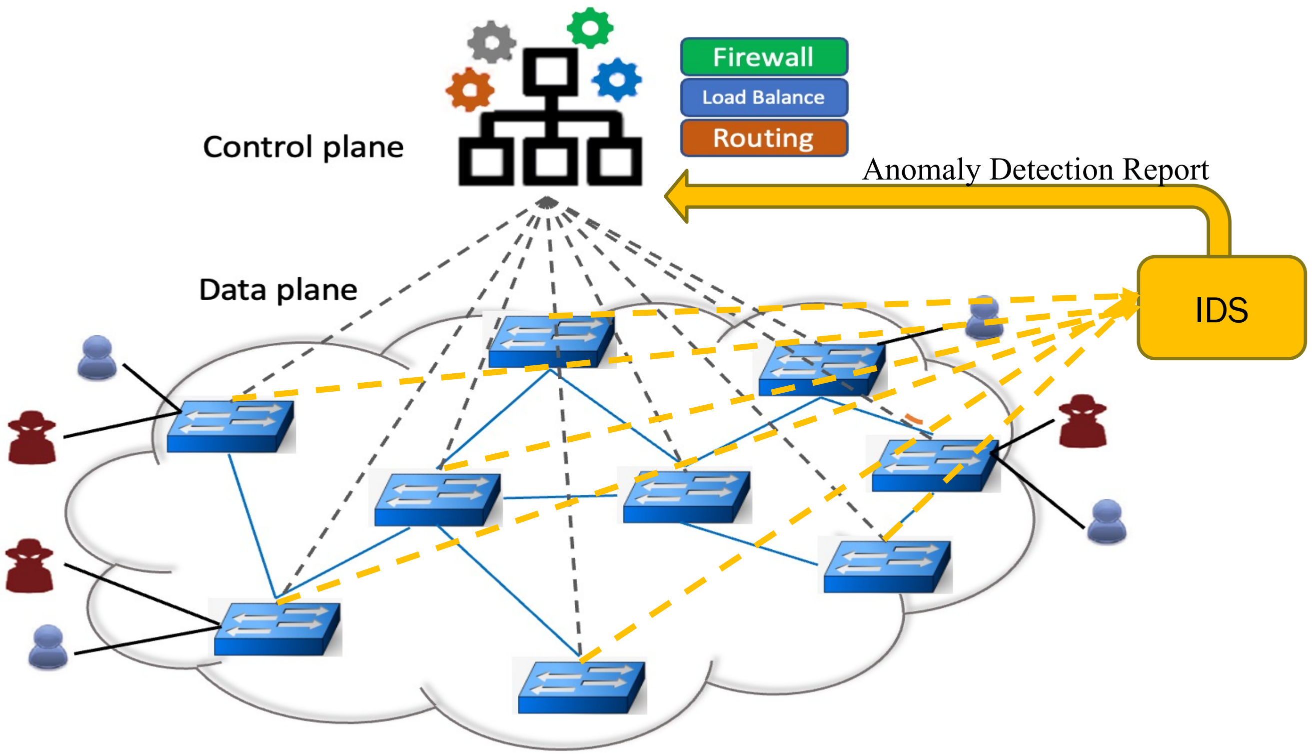
Intrusion Detection System Application

- Detect anomalies
- Drop flows
- Redirect flows



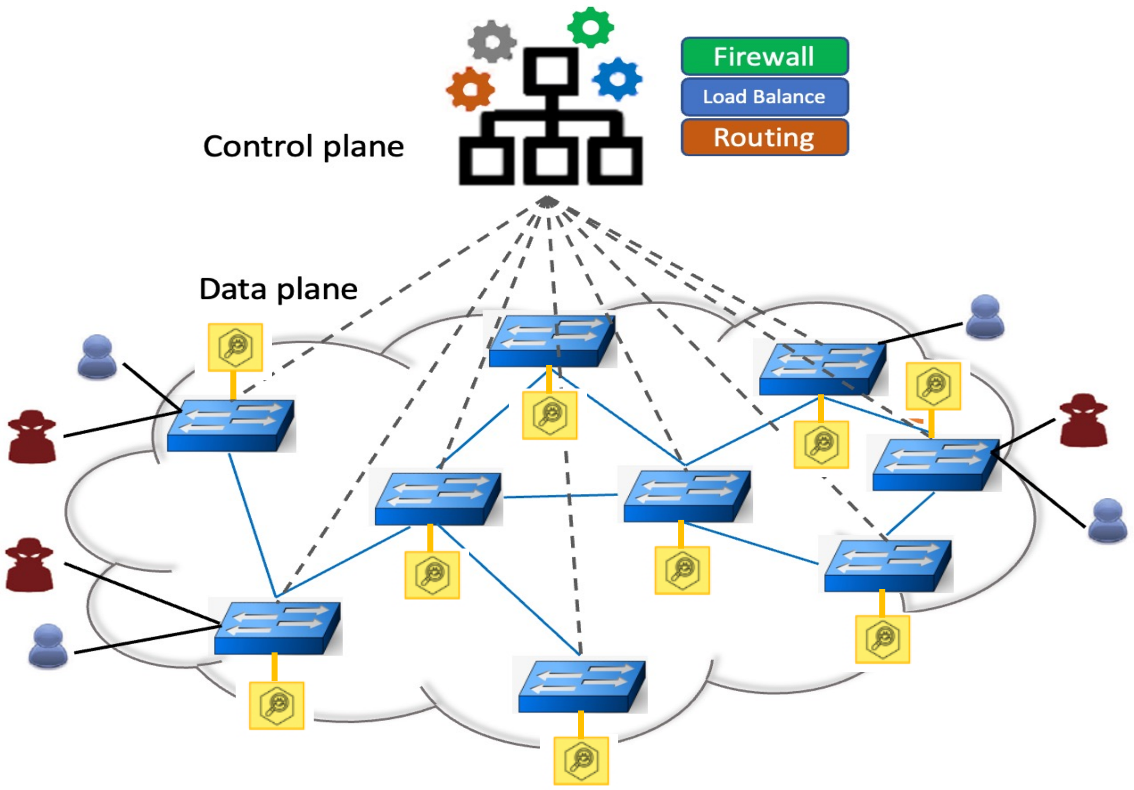
Centralized Intrusion Detection System in Data Plane

- Limited Capacity
- Overloading
- Delay

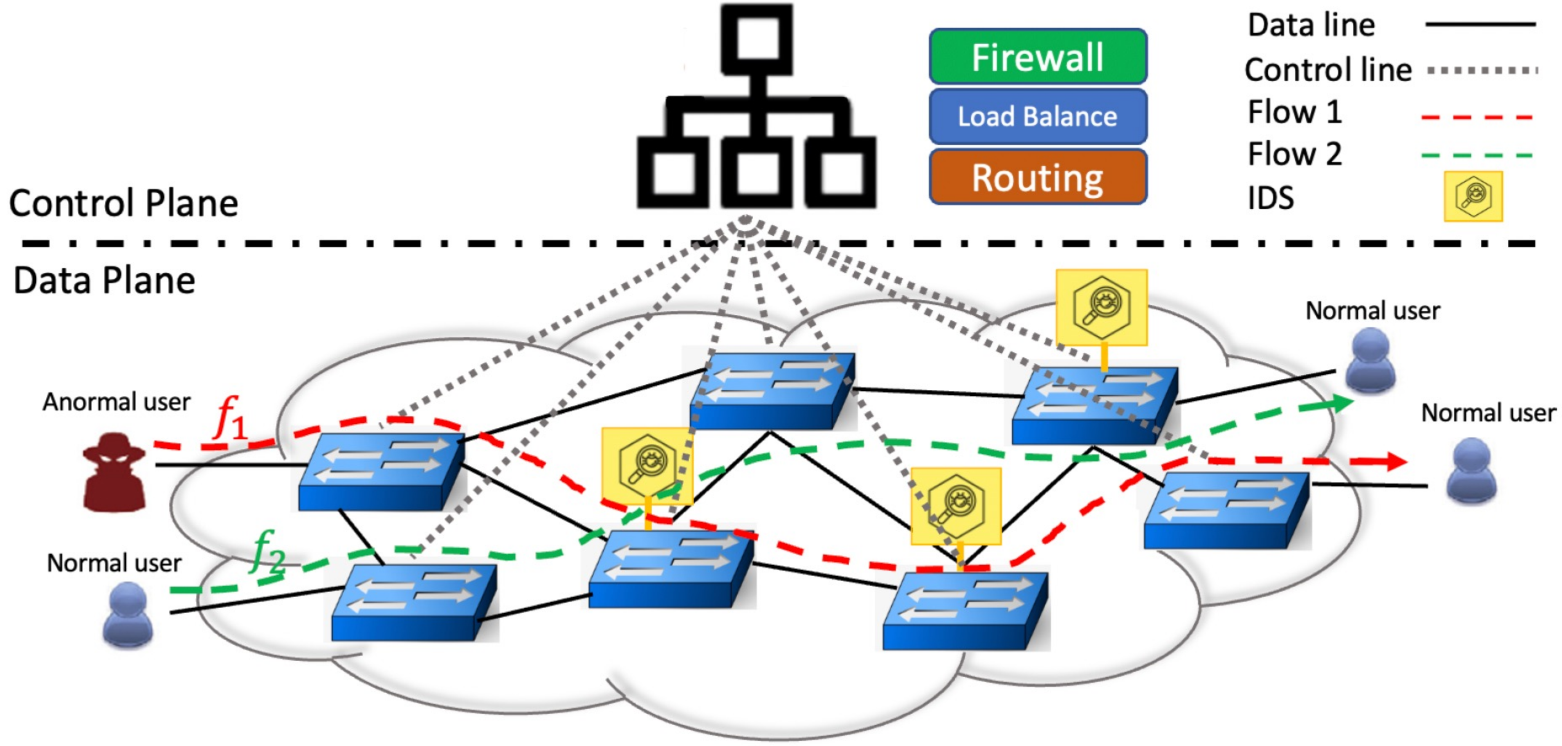


Intrusion Detection System for Switches in Data Plane

- Cost of installation
- Missing rate
- Limited Capacity



Chain of Intrusion Detection System in Data Plane



IDS has limited hardware resources in terms of CPU power, memory access speed, and storage capacity. IDS applications are unable to achieve an acceptable detection rate.

Chains of IDSs may provide a solution to this problem. How can multiple IDSs be implemented on the SDN?

Implementing an IDS chain can improve detection rates. Due to installation costs and flow table capacity limitations, IDS cannot be installed on all switches. Therefore, there are a limited number of IDSs. As incoming traffic is grouped, there is no need for many IDSs.

Which method is the best for grouping flows?

Grouping flows and IDS assigning techniques can have a significant impact on performance measurements, such as dropping rates under high load and transmission delays caused by non-shortest path routing.

How can we maintain balanced flow groups? How can flow groups be matched with IDS chains?

Proposed Method

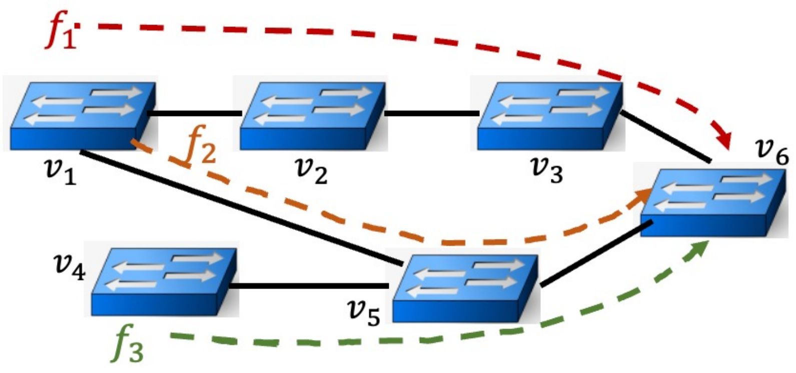
1. Provide chains of IDSs on the data plane to increase the rate of intrusion detection and reduce the dropping rate.

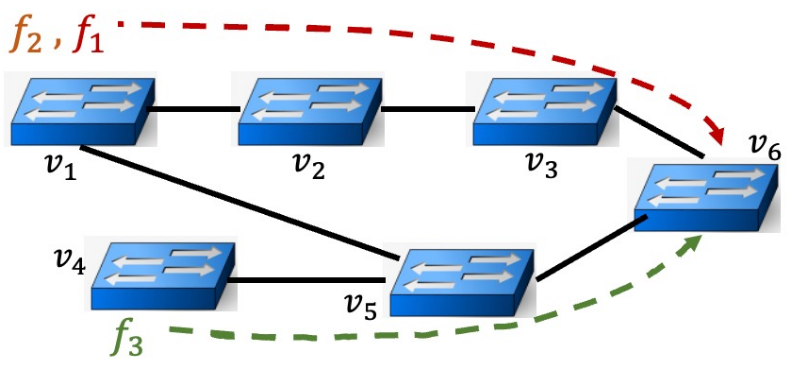
2. Introduce a creative centroid-based (modified K-means clustering method) to group the incoming flows.

3. Introduce two models for matching flow groups to IDS chain: minimum cost 2-D matching and minimum cost 3-D matching.

4. Evaluate the performance of our approach on a real test bed under different measurements.

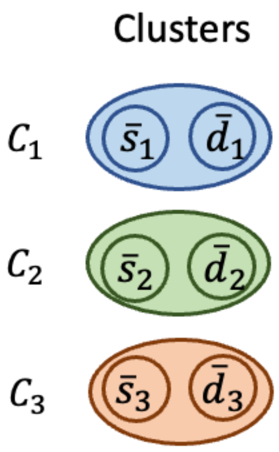
Grouping the Flows



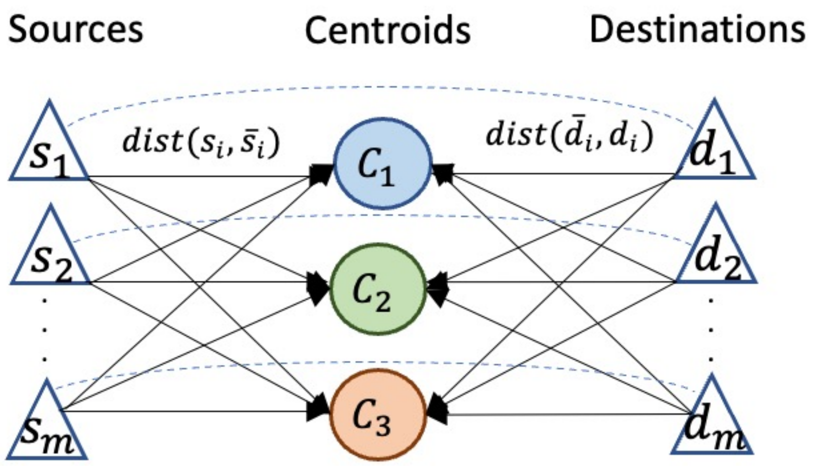


Grouping the Flows

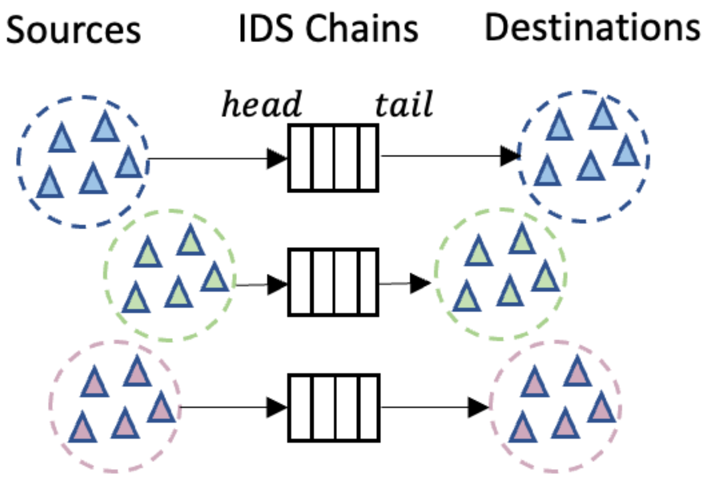
Virtual centroid



Grouping

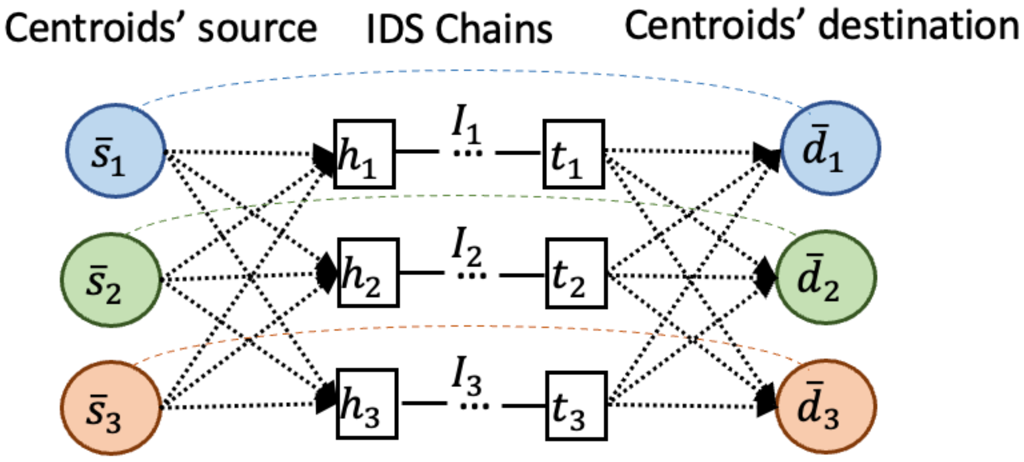


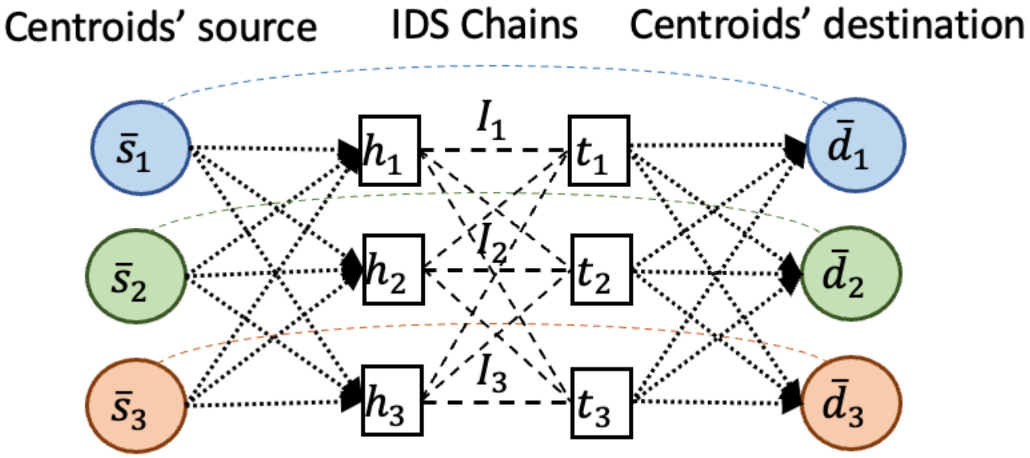
Matching



$$dis(s_i, \bar{s}_i) + dis(\bar{d}_i, d_i)$$

Matching Flow Groups to IDS chain





Problem 1. Grouping incoming traffic to reduce transmission delay in a balanced way. The distance of flows to the cluster's centroid and the total amount of traffic in each cluster are important factors that should be taken into consideration. This problem is NP-hard, and we provide an approximation based on the grouping of the incoming flows with the help of the modified version of K-means clustering. We formulate the grouping incoming traffic problem as an optimization problem with an objective of minimizing overhead/cost.

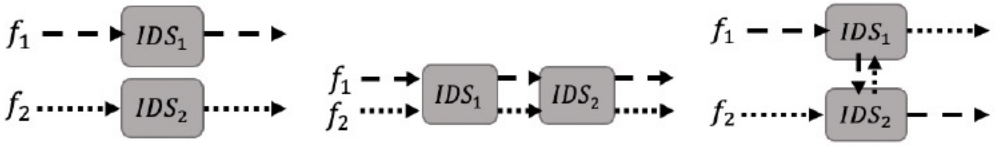
$$\begin{aligned} \min \quad & \sum\nolimits_{F_j \in F} cost(F_j) \\ \text{subject to} \quad & cost(F_j) = |F_j| \cdot \sum\nolimits_{f \in F_j} r_f \end{aligned}$$

Problem 2: Find an IDS chain assignment for each flow group so that the total number of malicious packets is minimized by ensuring that all the traffic is forwarded to an IDS chain before reaching the destination. We assume that the locations of IDS chains are predetermined. The problem can be expressed as the following:

$$\begin{aligned} \min \quad & \sum\nolimits_{i \in I} cost(I) \\ \text{subject to} \quad & cost(I) = \sum\nolimits_{M_{j,i}=1} R_j * \min dist(F_j, I_i) \\ & R_j = \sum\nolimits_{f \in F_j} r_f \\ & 1 \leq |I_i| \end{aligned}$$

Evaluation

- The rate of blocked malicious packets can be displayed by the detection rate!
- The rate of dropped malicious and legitimate packets can be displayed by the dropping rate!



(a) One IDS (b) Same IDS (c) Mixed IDS

TABLE II: Comparison of one IDS vs multiple IDSs

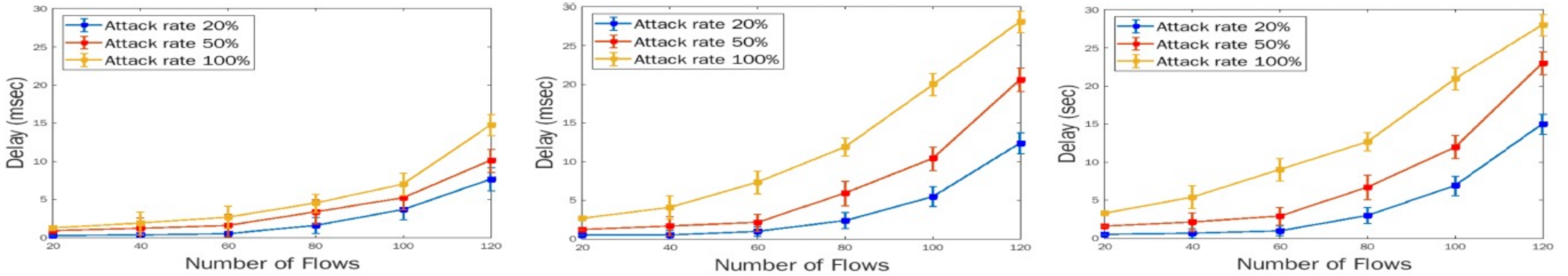
Traffic	Attack Rate	Detection Rate(%)			Dropping Rate(%)			Delay(msec)		
		Single	2 IDS	Mixed	Single	2 IDS	Mixed	Single	2 IDS	Mixed
Small	**20%**	36.6	48	52	24.9	26.3	25	1.8	3.45	3.3
	50%	47.5	55	60	25.5	26.9	26.2	3.6	6.9	6.45
	80%	52	69	72	24.8	26.7	25.1	6.1	11.31	10.8
Medium	**20%**	49.3	64.5	74.5	28.7	30.5	29.9	5.55	9.99	9.57
	50%	60.3	71	73	28	29.5	28.9	7.1	15	14.1
	80%	72	81	83	28.9	32	31.5	13.5	24.9	24.51
Large	**20%**	61.8	80.3	85	31.2	34	32.7	9.6	17.4	16.5
	50%	74.1	86	91	34.5	36.3	35.18	17.1	33.3	32.82
	80%	81	92	94.3	35	37.5	38.7	30	54.6	54

TABLE III: Effects of clustering methods on overhead and detection rate for an IDS chain with one IDS

Clustering Method	Overhead (%)	Detection Rate (%)	Delay (ms)
K-means and random assigning	21%	45%	2.7
K-means and total matching	27.5%	64.5%	3.33
K-means++ and total matching	31.2%	64.7%	4.1
Balanced K-means and total matching	35.7%	74%	6.32
Balanced K-means and partial matching	36%	81%	6.4

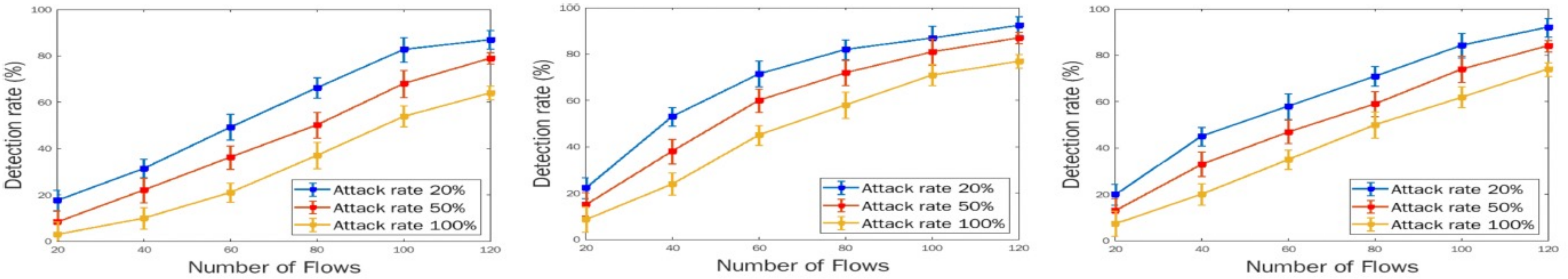
TABLE IV: Effects of IDS in control plane and data plane under different amounts of incoming traffic

Anomaly Detection	Ctr-Overhead(%)			Dropping Rate(%)			Detection Rate(%)			Delay (ms)		
	S	M	L	S	M	L	S	M	L	S	M	L
Centralized IDS	7	12	27	32.6	37	43.2	39.4	53.3	68.3	2.7	5.3	19.2
Chain with one IDS	10.2	12.3	17.8	31	28.5	33.8	38.5	60.3	74.1	3.6	7.1	23.1
Chain with two IDS	10.3	12.3	18	32.9	31.5	35.6	55	71	86	9.6	15	30.3



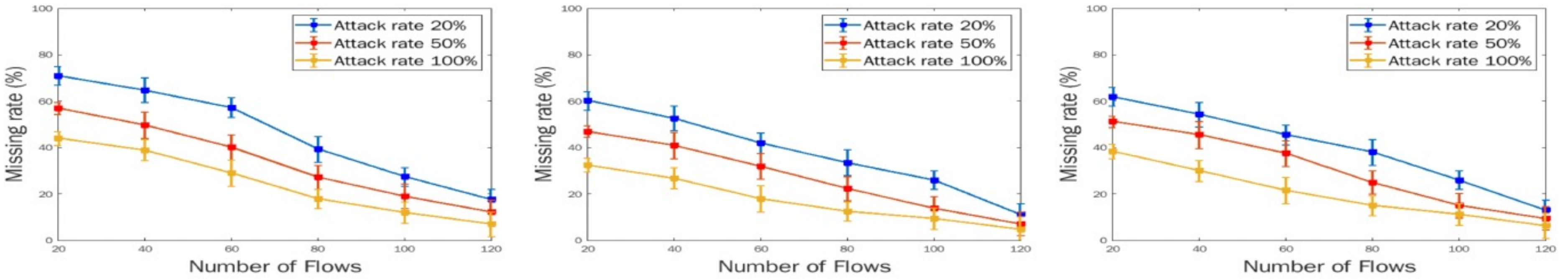
(a) One IDS (b) Multiple IDSs (c) Mixed IDS

Fig. 9: Delay time.



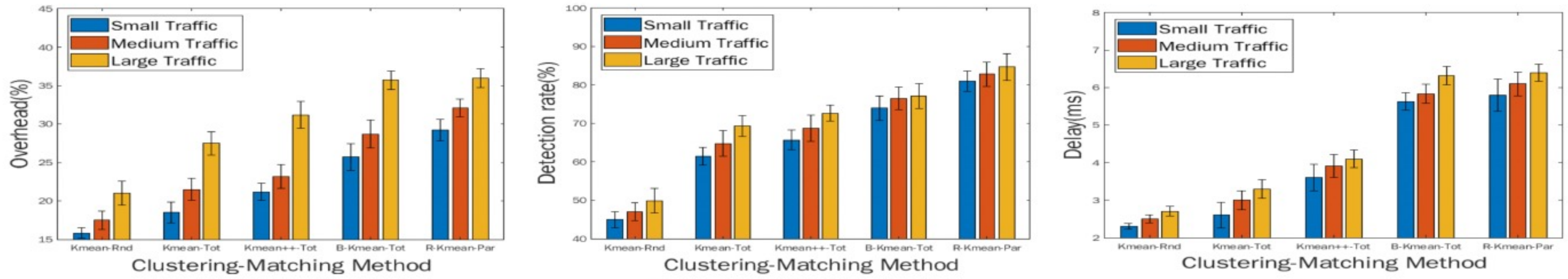
(a) One IDS (b) Multiple IDSs (c) Mixed IDS

Fig. 10: Detection rate.



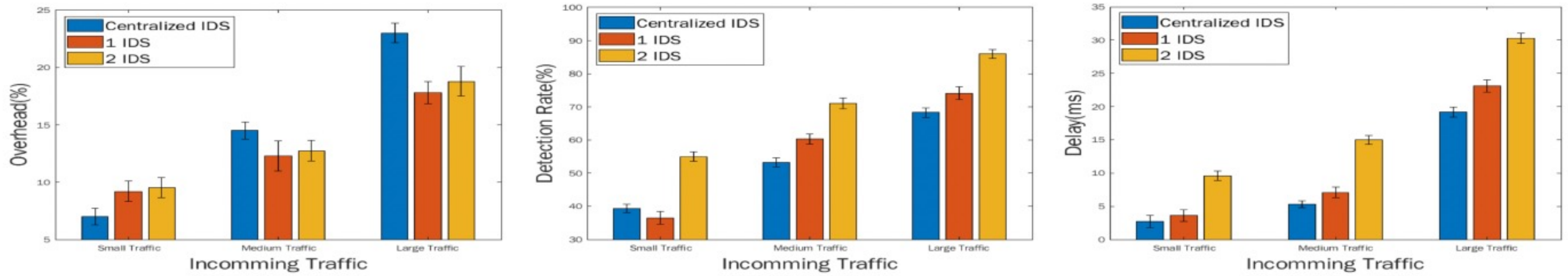
(a) One IDS (b) Multiple IDSs (c) Mixed IDS

Fig. 11: Missing rate.



(a) Overhead (b) Attack detection rate (c) Delay

Fig. 12: Detection rate, overhead, and delay for different clustering methods.



(a) Overhead (b) Attack detection rate (c) Delay

Fig. 13: Comparison between centralized IDS, 1 IDS, and 2 IDS for detection rate, overhead, and delay.

Summary

Since deploying a single IDS in network cannot handle the traffic with fast rate on time we proposed a mechanism to deploy multiple IDSs in network and separate the incoming traffic to multiple route paths.

With this process, traffic is load-balanced and IDS is capable to detect fewer packets to increase detection efficiency.

We tried to minimize the cost (the overhead of SDN controller) by grouping flows (separate flows to different paths) and improve IDS detection capability

We performed experiments to explore different patterns of IDS deployment and evaluated several factors such as detection rate, dropping rate, and delay time