NARLabs 國家實驗研究院

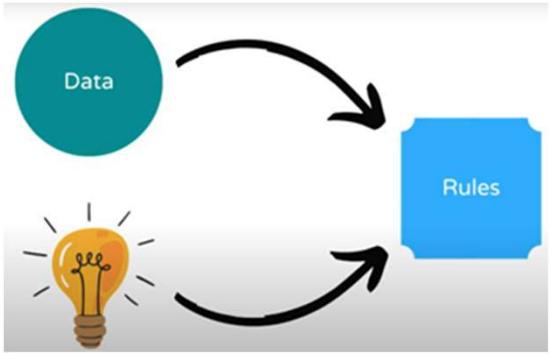
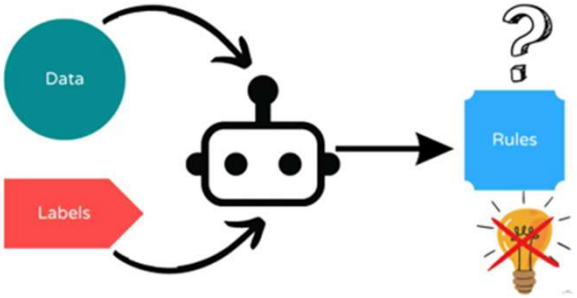
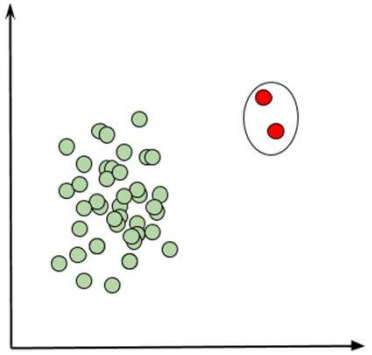
國家高速網路與計算中心

利用機器學習方法在TWAREN流量異常偵測

2023.07.13 李崇瑋

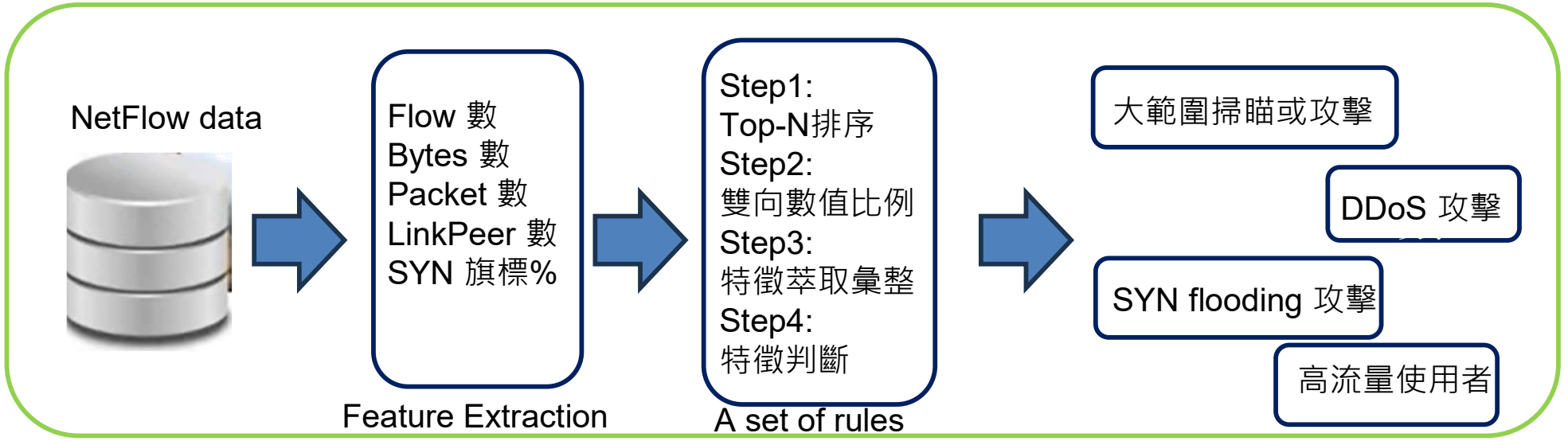
NARLabs

Backbone Network anomaly detection

Statistical & rule-based decision making	Supervised Learning Classification	Unsupervised Learning Outlier detection
		

Backbone Network anomaly detection

- Statistical & Rule-based



Statistical & Rule-based anomaly detection

異常類型	嚴重/異常超標
連線對象過多	『五分鐘內連線不同IP數高達379,690個』
疑似大範圍掃瞄或入侵	『目的Port共65596個』
疑似SYN攻擊	『SYN比例超過95%』
輸出流量過高 Bytes 量太多	異常超標：『用量41,000MB（40/40,959）高達全網7.21%
封包數量超級多	『封包數61,874,270（0/61,874,270）高達全網2.27%』

TWAREN骨幹異常使用即時偵測與告警系統

論文 | Theses

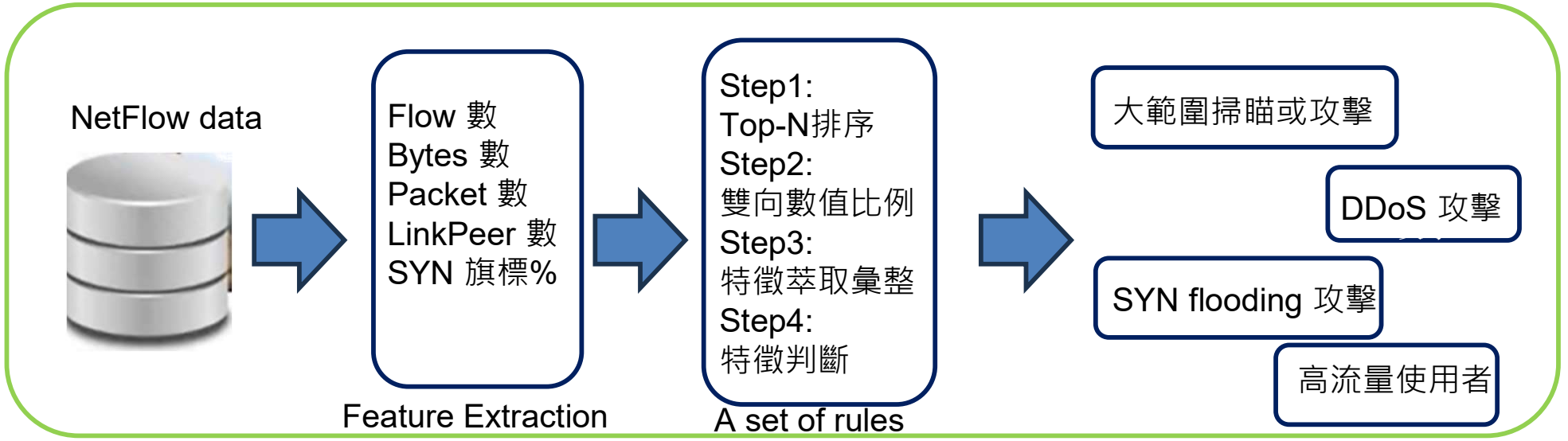
發表日期 最近更新日期 ~ 查詢

序號	論文名稱	發表者	會議名稱	發表日期	最近更新日期	下載次數
1	運用大數據，偵測SSH字典攻擊告警分析系統	陳品瑄 梁明章 陳俊傑	第十六屆離島資訊技術與應用研討會	2017/5/20		2634
2	Heterogeneous Interconnection between SDN and Layer2 Networks based on NSI	周大源,黃文源, 李慧蘭,劉德隆	Advanced Information Networking and Applications (AINA-2017)	2017/3/28		2747
3	TWAREN網路效能量測應用於0815停電之監控	楊哲男, 古立其, 陳俊傑, 呂宗翰,	2017台灣網際網路研討會	2017/10/27		2374
4	TWAREN骨幹異常使用即時偵測與告警系統	梁明章	2017台灣網際網路研討會	2017/10/26		2238

https://noc.twaren.net/noc_2008/Download/Theses_index.php?page=5

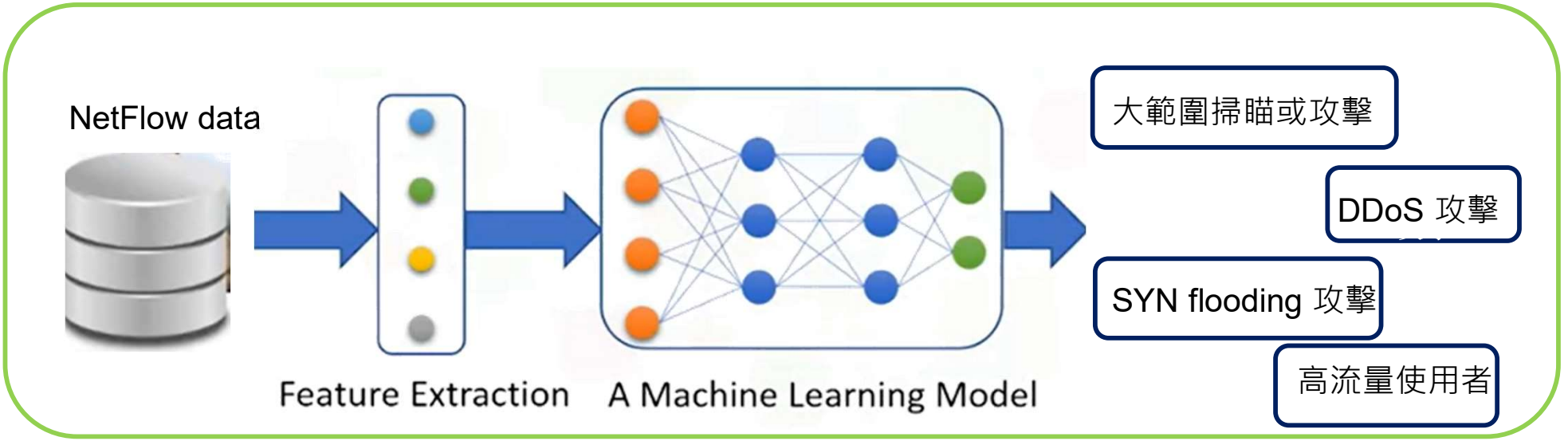
Backbone Network anomaly detection

- Statistical & Rule-based



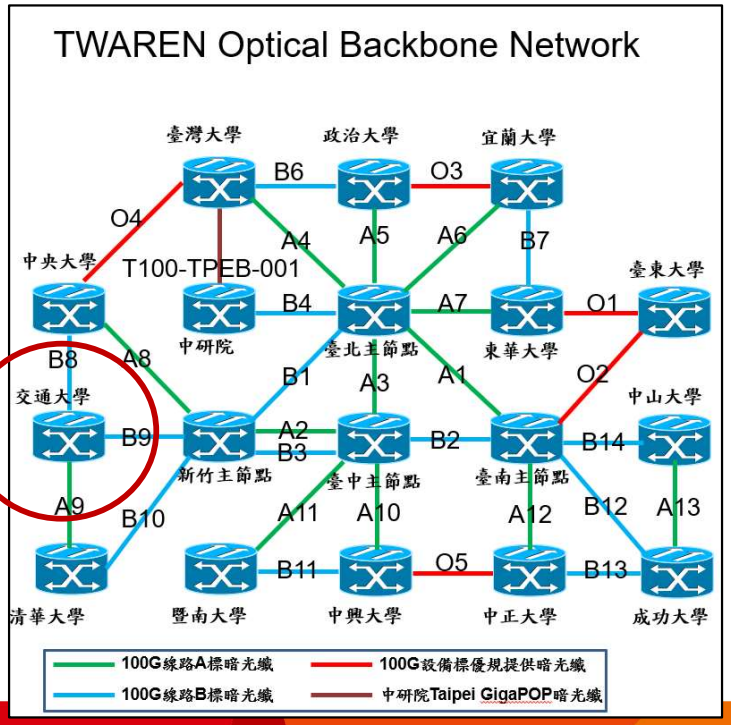
Backbone Network anomaly detection

- Machine Learning Classification

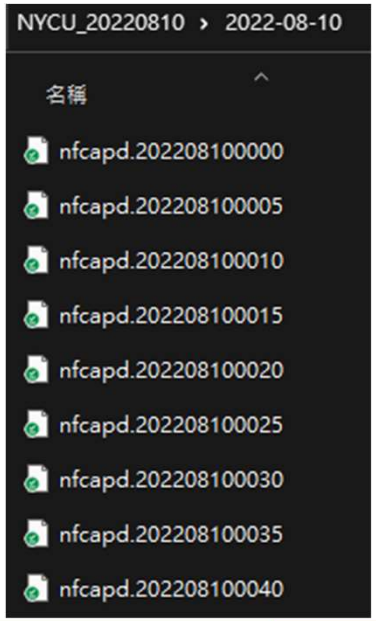


Data Preparation

- NCTU NetFlow from 00:00 to 23:50 on 8/10 (27 million records、844MB)
- integrate the current attacker IP labels into the model training process.



X → Y



IP	NccstKind	NccstType	Recommendation
185.156.73.100	INT入侵攻擊情資	對外攻擊	1.檢查出口資安設備是否記錄到異常資訊
92.63.197.61	INT入侵攻擊情資	對外攻擊	1.檢查出口資安設備是否記錄到異常資訊
185.156.73.63	INT入侵攻擊情資	對外攻擊	1.檢查出口資安設備是否記錄到異常資訊
89.248.165.169	INT入侵攻擊情資	對外攻擊	1.檢查出口資安設備是否記錄到異常資訊
89.248.163.140	INT入侵攻擊情資	對外攻擊	1.檢查出口資安設備是否記錄到異常資訊
185.156.73.100	INT入侵攻擊情資	對外攻擊	1.檢查出口資安設備是否記錄到異常資訊
92.63.197.61	INT入侵攻擊情資	對外攻擊	1.檢查出口資安設備是否記錄到異常資訊
89.248.165.60	INT入侵攻擊情資	對外攻擊	1.檢查出口資安設備是否記錄到異常資訊
89.248.163.140	INT入侵攻擊情資	對外攻擊	1.檢查出口資安設備是否記錄到異常資訊
146.196.52.26	INT入侵攻擊情資	對外攻擊	1.檢查出口資安設備是否記錄到異常資訊
89.248.165.205	INT入侵攻擊情資	對外攻擊	1.檢查出口資安設備是否記錄到異常資訊
92.63.197.61	INT入侵攻擊情資	對外攻擊	1.檢查出口資安設備是否記錄到異常資訊
89.248.165.60	INT入侵攻擊情資	對外攻擊	1.檢查出口資安設備是否記錄到異常資訊
89.248.164.165	INT入侵攻擊情資	對外攻擊	1.檢查出口資安設備是否記錄到異常資訊
89.248.165.218	INT入侵攻擊情資	對外攻擊	1.檢查出口資安設備是否記錄到異常資訊
185.156.73.63	INT入侵攻擊情資	對外攻擊	1.檢查出口資安設備是否記錄到異常資訊
103.74.122.45	INT入侵攻擊情資	對外攻擊	1.檢查出口資安設備是否記錄到異常資訊
89.248.164.165	INT入侵攻擊情資	對外攻擊	1.檢查出口資安設備是否記錄到異常資訊
94.102.61.2	INT入侵攻擊情資	對外攻擊	1.檢查出口資安設備是否記錄到異常資訊
89.248.165.82	INT入侵攻擊情資	對外攻擊	1.檢查出口資安設備是否記錄到異常資訊
89.248.165.205	INT入侵攻擊情資	對外攻擊	1.檢查出口資安設備是否記錄到異常資訊

Feature Engineering

- Select 9 out of the 48 available features in the NetFlow data

ts	2022/8/9 23:59	2022/8/9 23:59	2022/8/9 23:59
te	2022/8/9 23:59	2022/8/9 23:59	2022/8/9 23:59
td	0	0.3	0
sa	2600:1900:4110:ba3::	2600:1900:4110:ba3::	2001:288:4001:d791:c0b3:2cb0:906a:cd4e
da	2804:60d4:300:221::5	2804:60d4:300:221::5	2a00:86c0:2062:2062::148
sp	443	443	57105
dp	55445	34368	443
pr	TCP	UDP	TCP
flg	...A...F	.....	...A....
fwd	64	64	64
stos	0	0	0
ipkt	1	2	1
ibyt	72	142	61
opkt	0	0	0
obyt	0	0	0
in	35	35	35
out	127	127	127
sas	15169	15169	1659
das	269194	269194	2906
smk	31	31	34
dmk	32	32	48
dtos	0	0	0
dir	0	0	0
nh	0.0.0.0	0.0.0.0	0.0.0.0
nhb	::	::	::
svln	0	0	0
dvln	0	0	0
ismc	00:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00
odmc	00:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00
idmc	00:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00
osmc	00:00:00:00:00:00	00:00:00:00:00:00	00:00:00:00:00:00
mpls1	0-0-0	0-0-0	0-0-0
mpls2	0-0-0	0-0-0	0-0-0
mpls3	0-0-0	0-0-0	0-0-0
mpls4	0-0-0	0-0-0	0-0-0
mpls5	0-0-0	0-0-0	0-0-0
mpls6	0-0-0	0-0-0	0-0-0
mpls7	0-0-0	0-0-0	0-0-0
mpls8	0-0-0	0-0-0	0-0-0
mpls9	0-0-0	0-0-0	0-0-0
mpls10	0-0-0	0-0-0	0-0-0
cl	0	0	0
sl	0	0	0
al	0	0	0
ra	211.73.76.15	211.73.76.15	211.73.76.15
eng	0/0	0/0	8/129
exid	1	1	1
tr	00:00.1	00:00.1	00:00.1

- `ts`: timestamp of the network traffic flow
- `sa`: source IP address
- `da`: destination IP address
- `dp`: destination port number
- `pr`: protocol (e.g. TCP, UDP, ICMP)
- `flg`: TCP flags
- `ipkt`: number of packets in the flow
- `ibyt`: number of bytes in the flow
- `dir`: flow direction (0 for outgoing, 1 for incoming)

Visualization of the GNN model

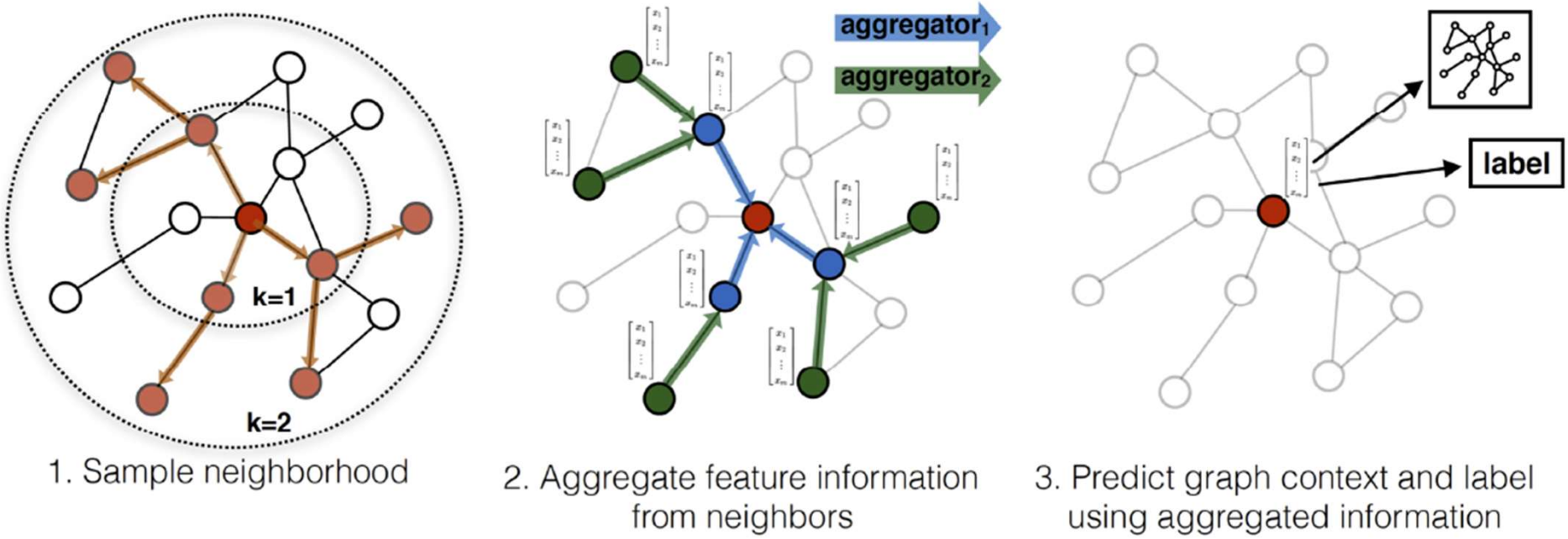


Figure 1: Visual illustration of the GraphSAGE sample and aggregate approach.

W. Hamilton, Z. Ying, and J. Leskovec, "**Inductive representati on learningon large graphs**,"
in Advances in Neural Information Processing Systems,vol. 30. Red Hook, NY, USA: Curran Associates, 2017.

GNN: Why?

✓ Example: テセウスの船

Name

Feature

Who is the murderer?

GNN: Why?

✓ We can train a classifier

$f($ 

$) = False$

$f($ 

$) = False$

$f($ 

$) = False$

$f($ 

$) = ?$

GNN: Why?

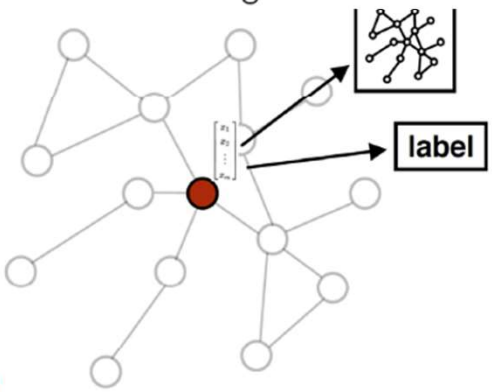
✓ The data may have underlying structure and relationship

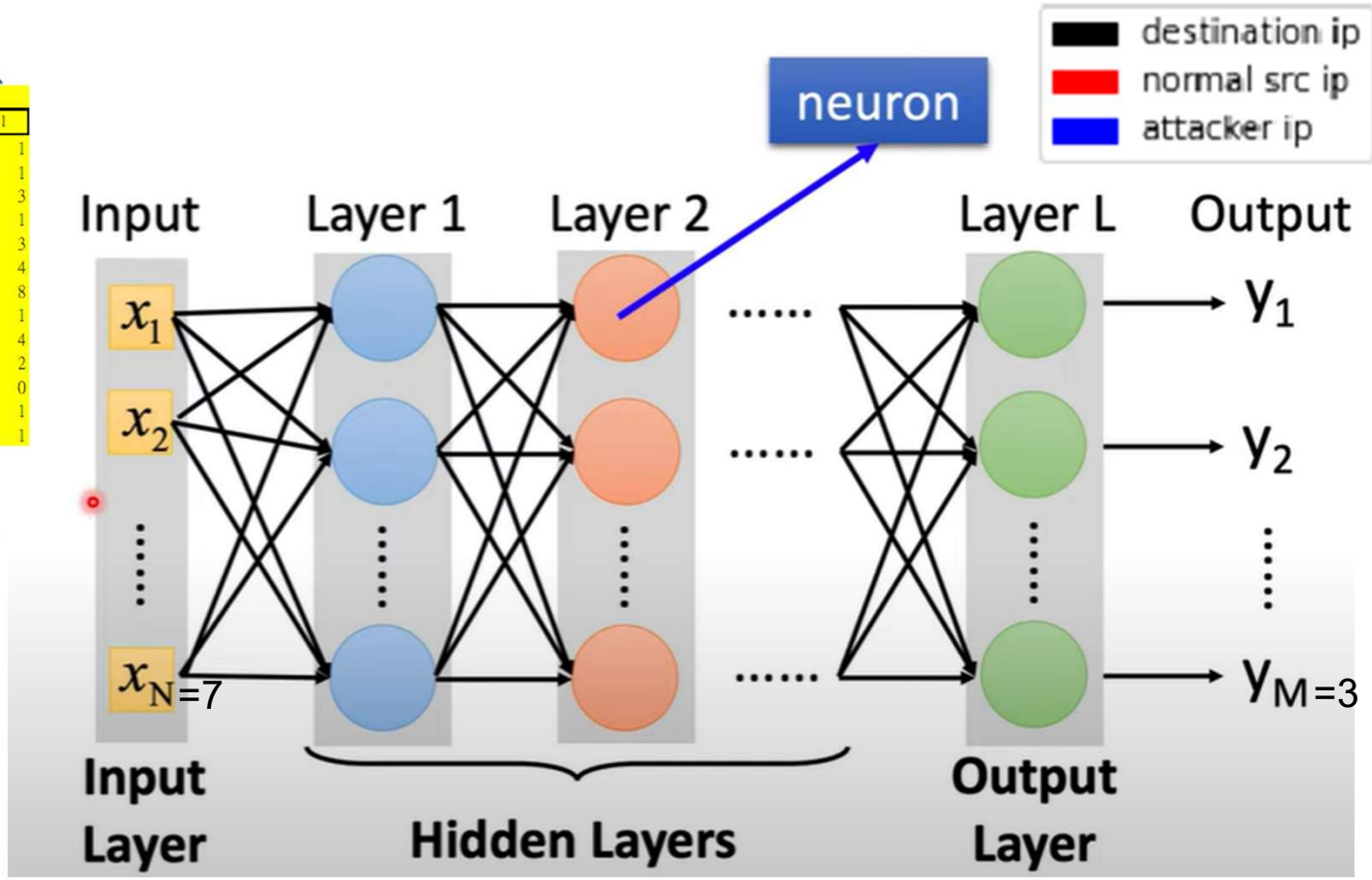
GNN Architecture

node features * 7

da_addr	pr	flg	dir	ipkt	ibyt	flows
10	1	1	1	1	40	1
1	1	1	1	1	40	1
1	1	0	1	1	56	1
3	1	0	1	3	168	3
1	1	12	1	3	249	1
3	1	0	1	4	244	3
4	1	0	1	6	366	4
1	1	0	1	13	1144	8
1	1	1	1	1	40	1
4	1	1	1	4	160	4
2	1	1	1	2	80	2
0	0	0	0	0	0	0
1	1	1	1	1	52	1
1	1	1	1	1	40	1

Aggregate feature information from neighbors





* One hidden layer with 13 channels

Classification Result by GNN model

Result

- Training accuracy is 0.988 , Training F1 score is 0.985
- Testing accuracy is **0.990**, Testing F1 score is **0.988**

Confusion matrix of Training

	dst ip	normal	attacker
dst ip	1693	0	0
normal	0	953	25
attacker	0	28	1500

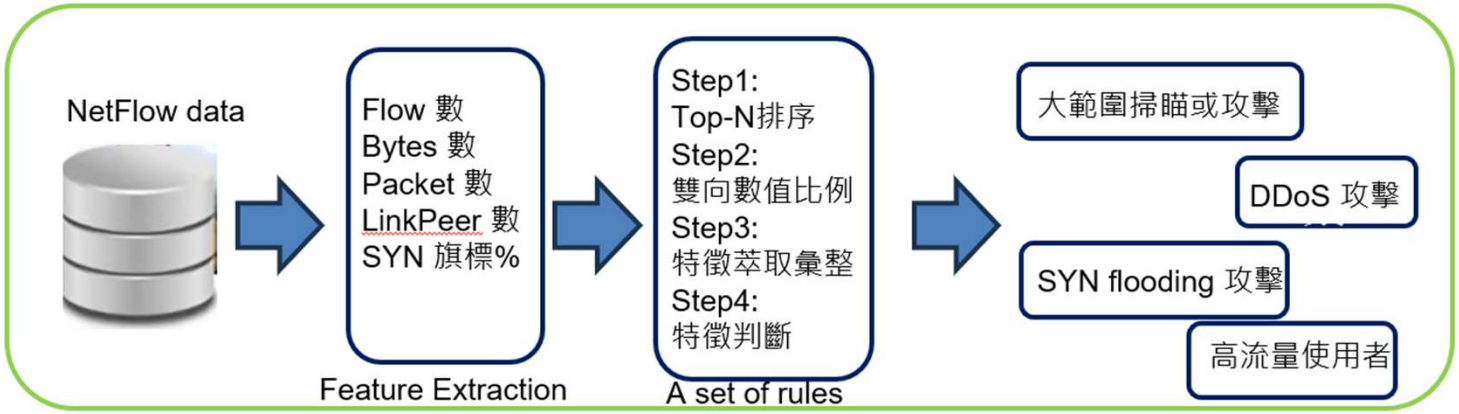
Confusion matrix of Testing

	dst ip	normal	attacker
dst ip	400	0	0
normal	0	202	6
attacker	0	3	312

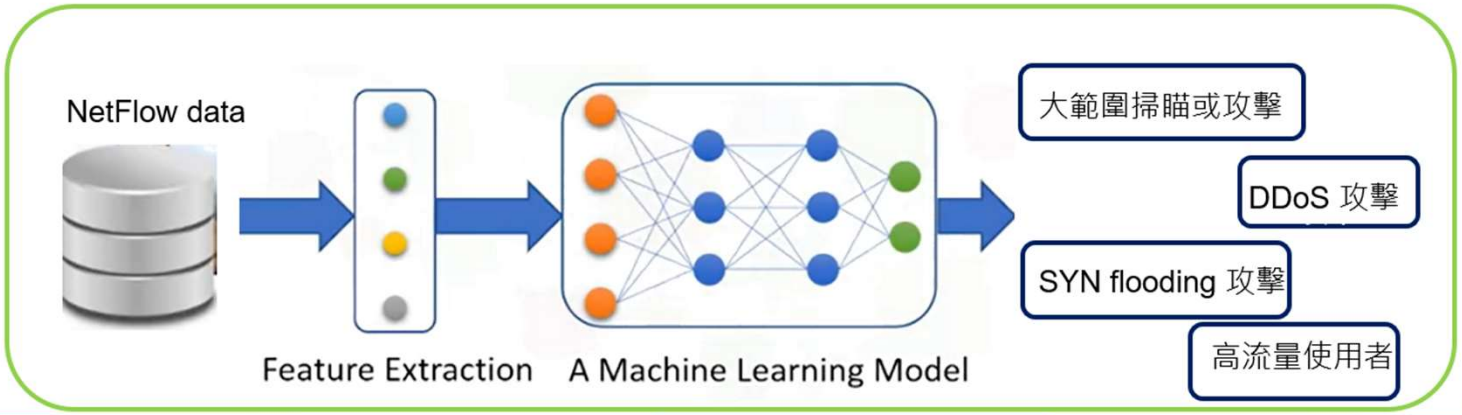
- both the testing accuracy and F1 score approach 99%.

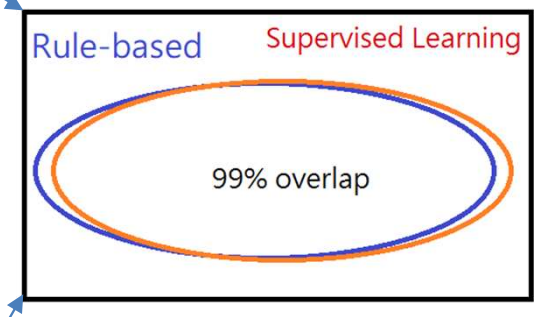
Supervised Learning Constrain

- Statistical & Rule-based Classification

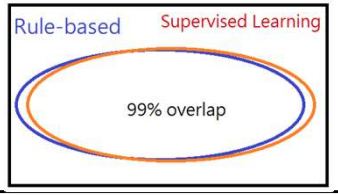


- Supervised Learning Classification





Supervised Learning Classification

Label Source	From current NCHC rule-based Result	From public NIDS Datasets
Pros	Achieved a testing accuracy of 99% from GNN model . Confusion matrix of Testing dst ip: 400, 0, 0 normal: 0, 202, 6 attacker: 0, 3, 312	a wider range of attack types label for training Table 7: NF-UQ-NIDS-v2 distribution Benign 25165295 / Scanning 3781419 DDoS 21748351 / Fuzzers 22310 Reconnaissance 2633778 / Backdoor 18978 Injection 684897 / Bot 143097 DoS 17875585 / Generic 16560 Brute Force 123982 / Analysis 2299 Password 1153323 / Shellcode 1427 XSS 2455020 / MITM 7723 Infilteration 116361 / Worms 164 Exploits 31551 / Ransomware 3425 Theft 2431
Cros	The performance of the classification is constrained by the labels that rely on established rules and assumptions. 	The publicly available NIDS datasets primarily consist of packet-based features, making them incomparable to the current NetFlow data collected by NCHC. NUM_PKTS_UP_TO_128_BYTES: Packets whose IP size <= 128 NUM_PKTS_128_TO_256_BYTES: Packets whose IP size > 128 and <= 256 NUM_PKTS_256_TO_512_BYTES: Packets whose IP size > 256 and <= 512 NUM_PKTS_512_TO_1024_BYTES: Packets whose IP size > 512 and <= 1024

NetFlow Data Source (PCAP Files / nfcapd Files)

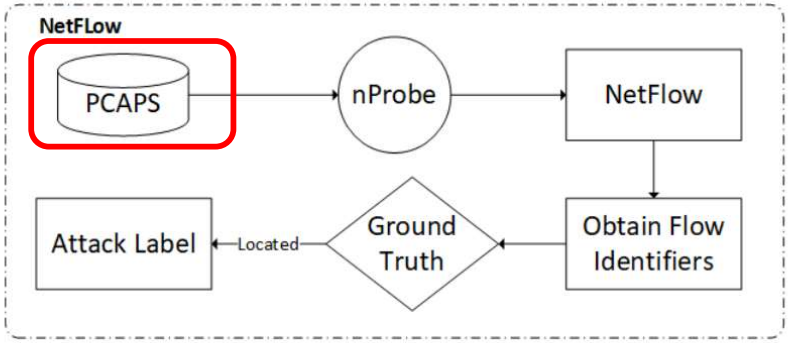
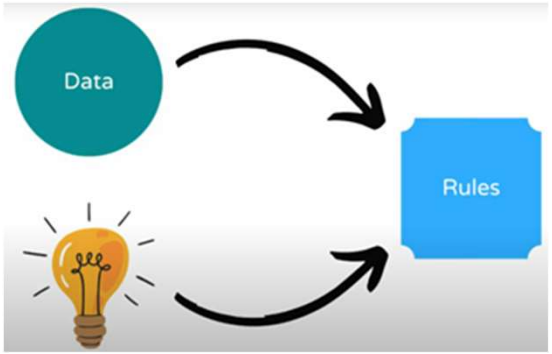
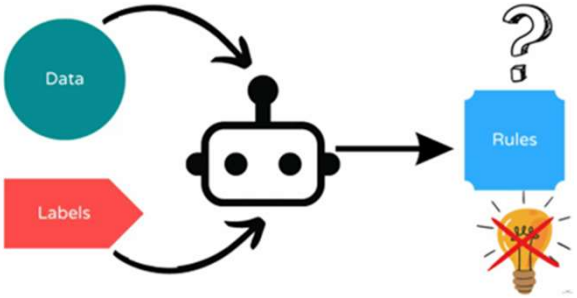
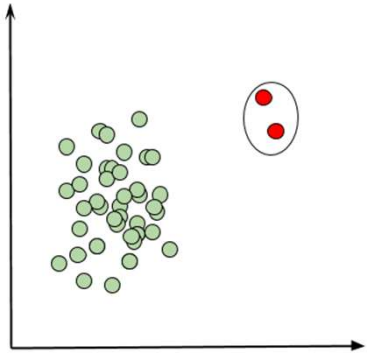


Fig. 2: Feature set extraction and labelling procedure

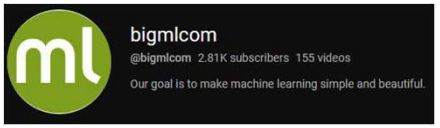
Aspect	PCAP Files	nfcapd Files
Format	Follow the libpcap file format	Specific to NetFlow, created by nfcapd daemon
Data Content	Individual packets, headers, payload	Aggregated flow data (source, destination IPs, ports, byte counts, timestamps, etc.)
Usage	Network troubleshooting	Network traffic analysis, capacity planning, billing, security monitoring
Analysis Tools	Wireshark, tcpdump	nfdump

Backbone Network anomaly detection

Statistical & rule-based decision making	Supervised Learning Classification	Unsupervised Learning Outlier detection
		

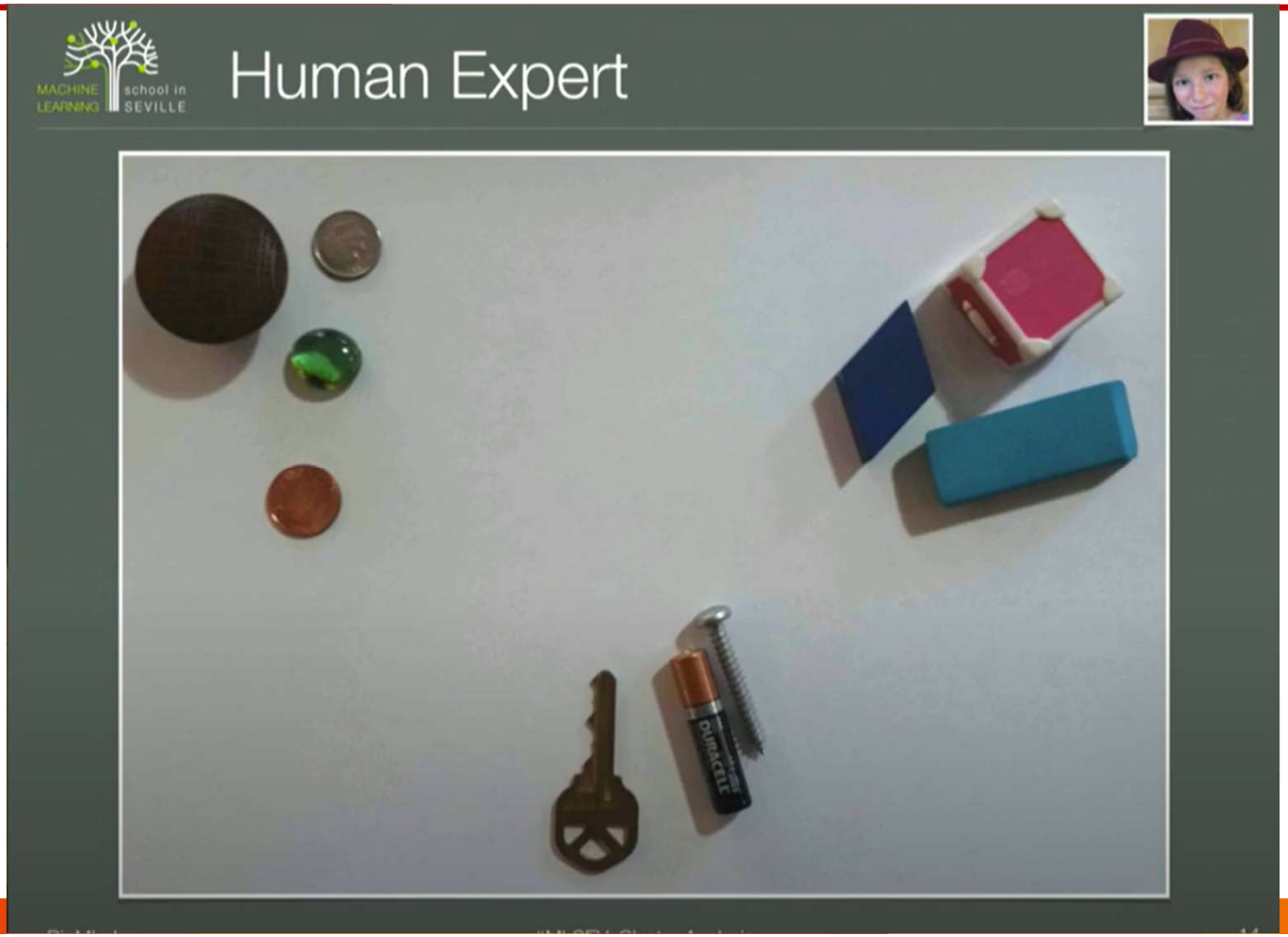
NARLabs

Cluster Analysis and Anomaly Detection

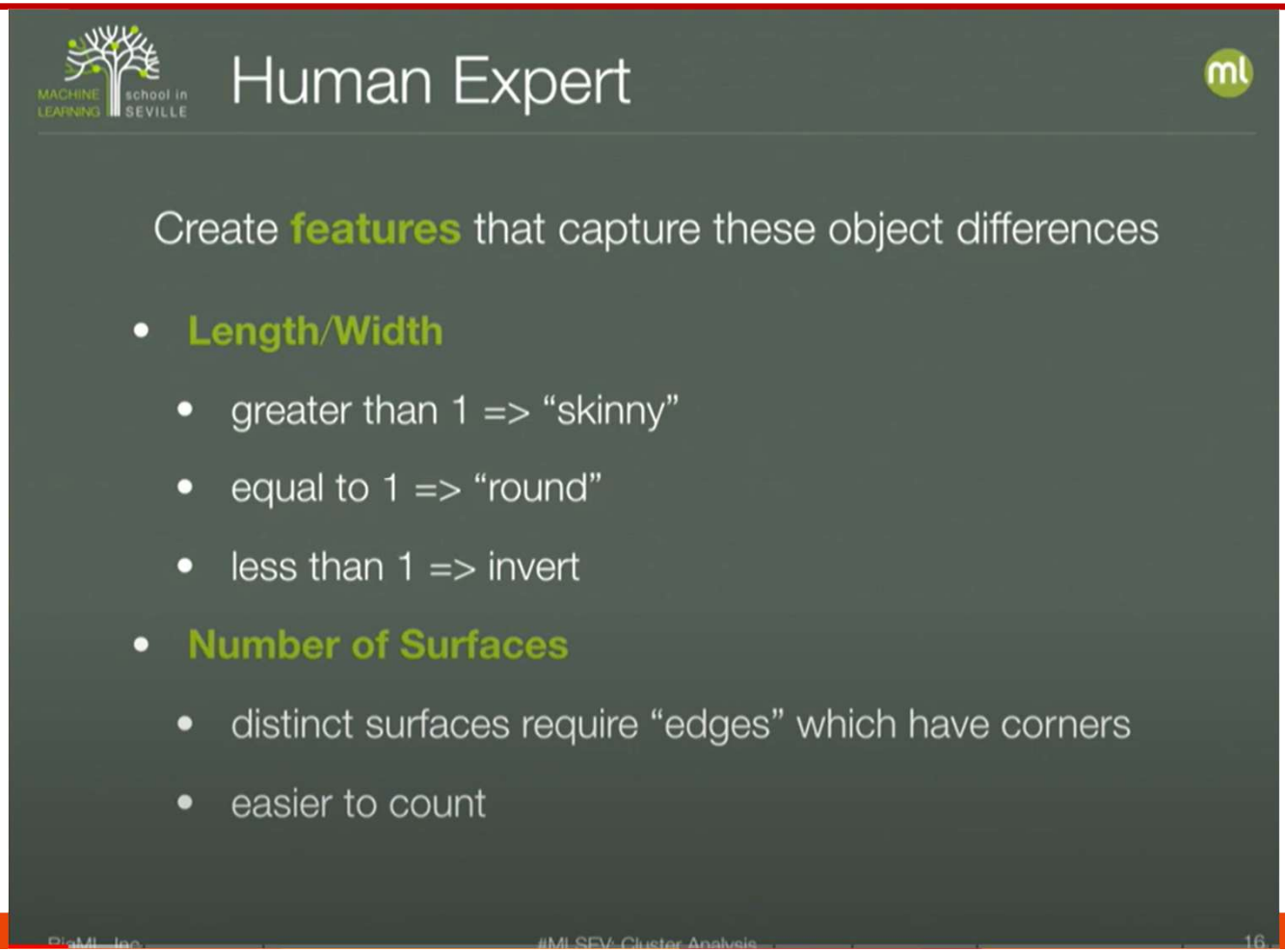


NARLabs

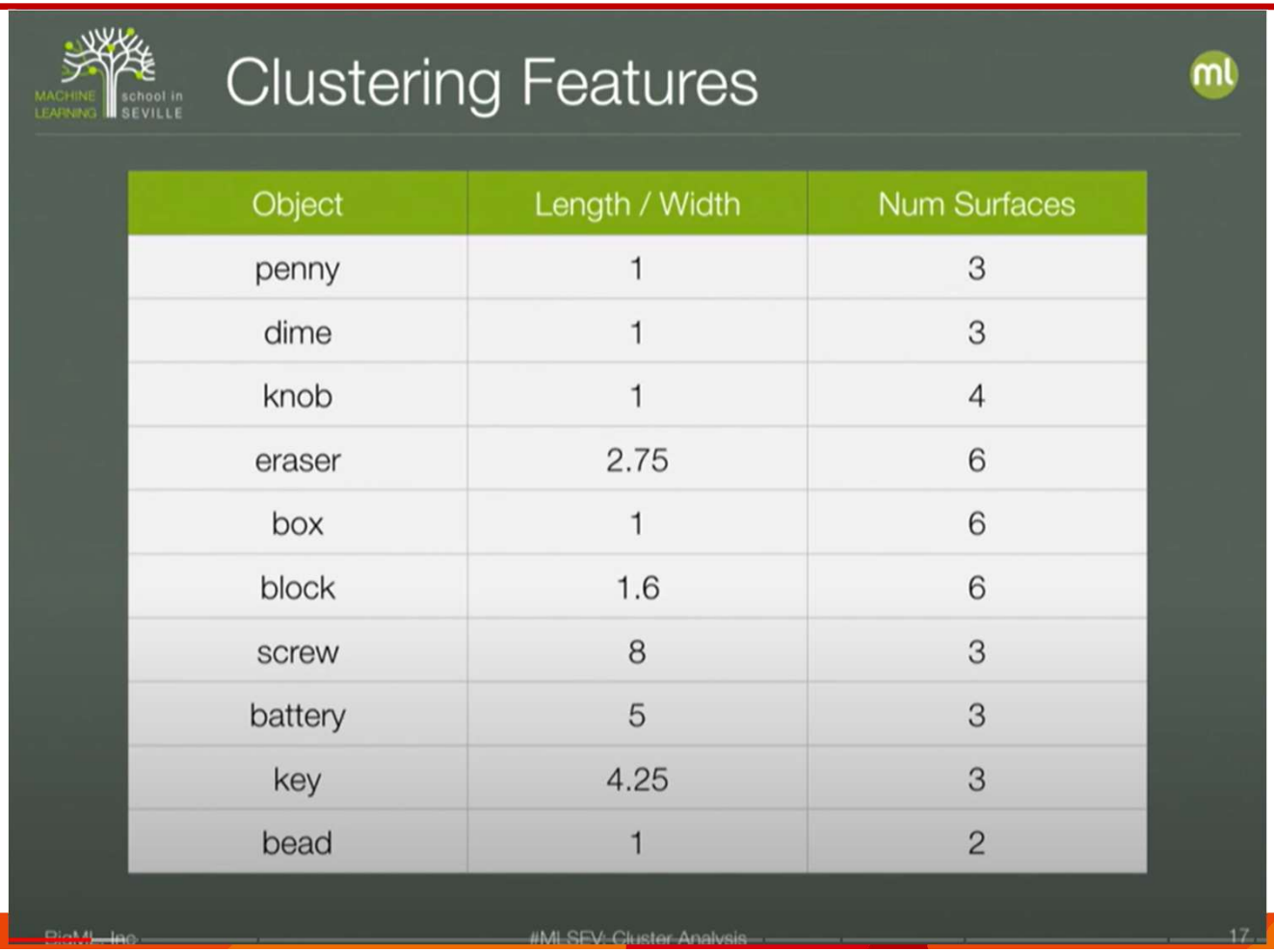
Cluster Analysis and Anomaly Detection



Cluster Analysis and Anomaly Detection



Cluster Analysis and Anomaly Detection

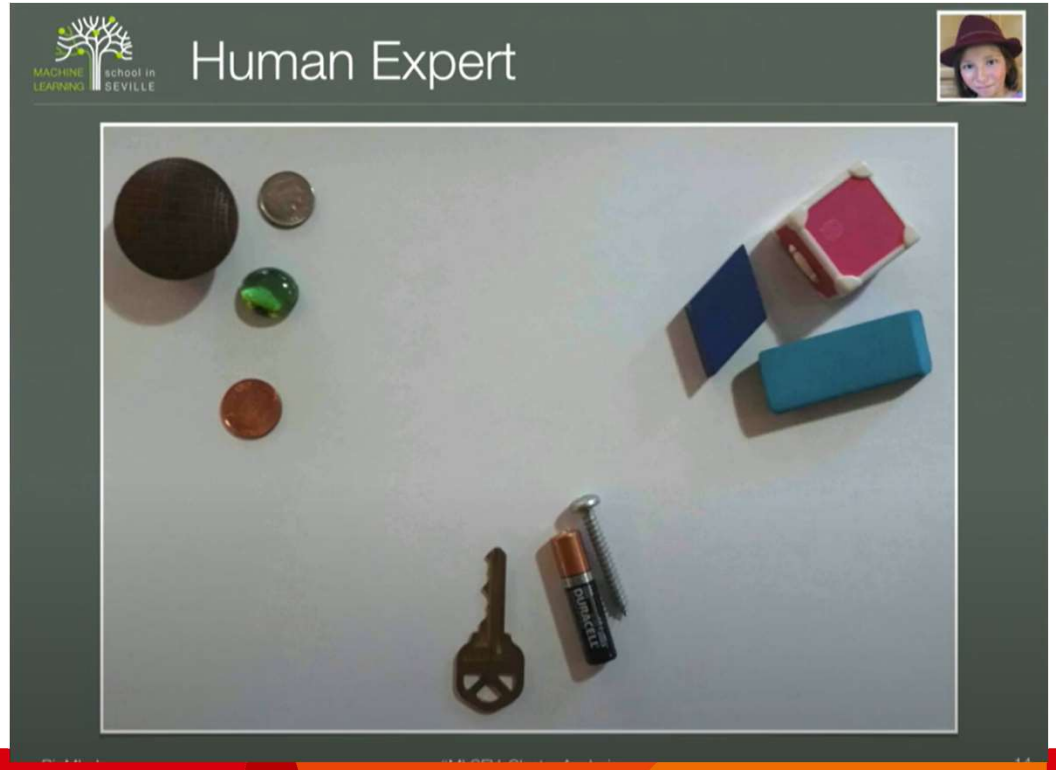


Object	Length / Width	Num Surfaces
penny	1	3
dime	1	3
knob	1	4
eraser	2.75	6
box	1	6
block	1.6	6
screw	8	3
battery	5	3
key	4.25	3
bead	1	2

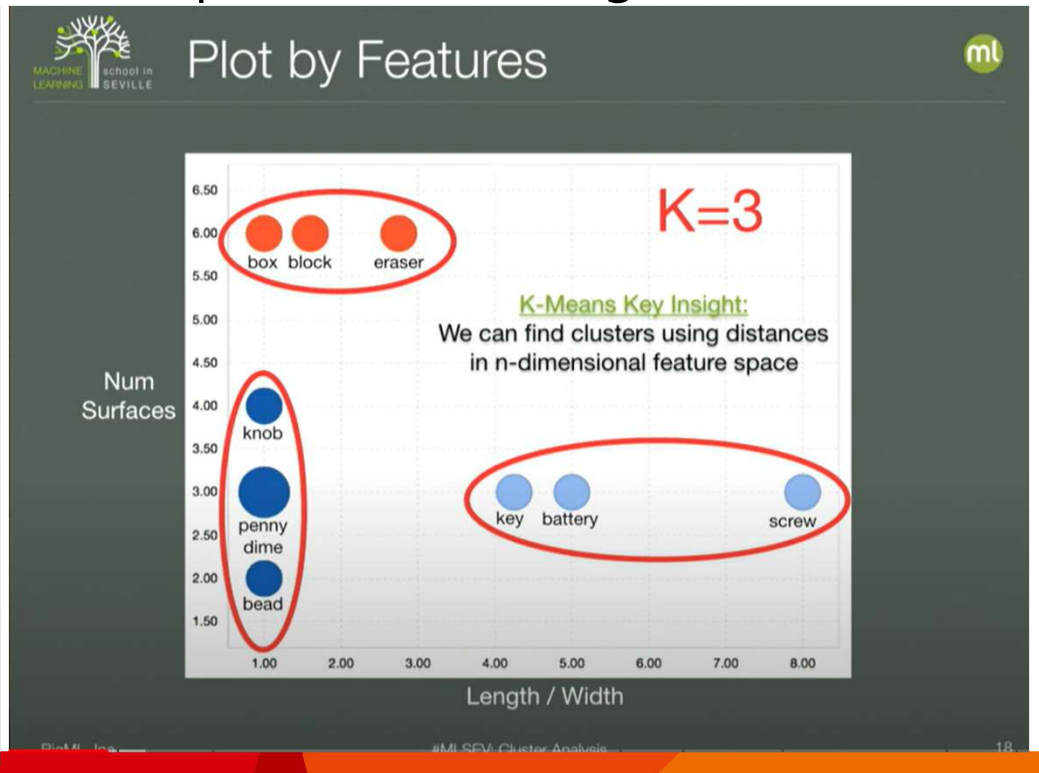
NARLabs

Cluster Analysis and Anomaly Detection

◆ Human



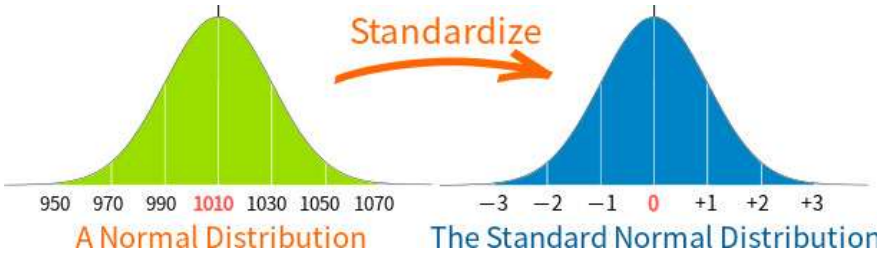
◆ Unsupervised Learning (Cluster)

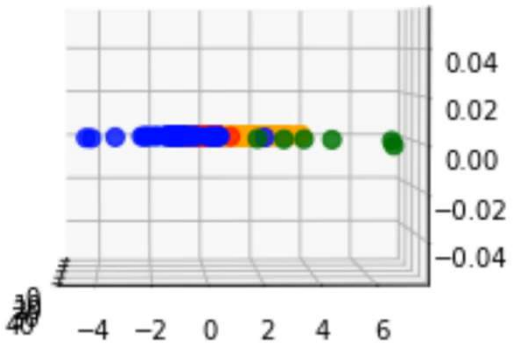


Feature Engineering & Clustering

numbers of peer links 、 packet count 、Bytes 、 Flow count

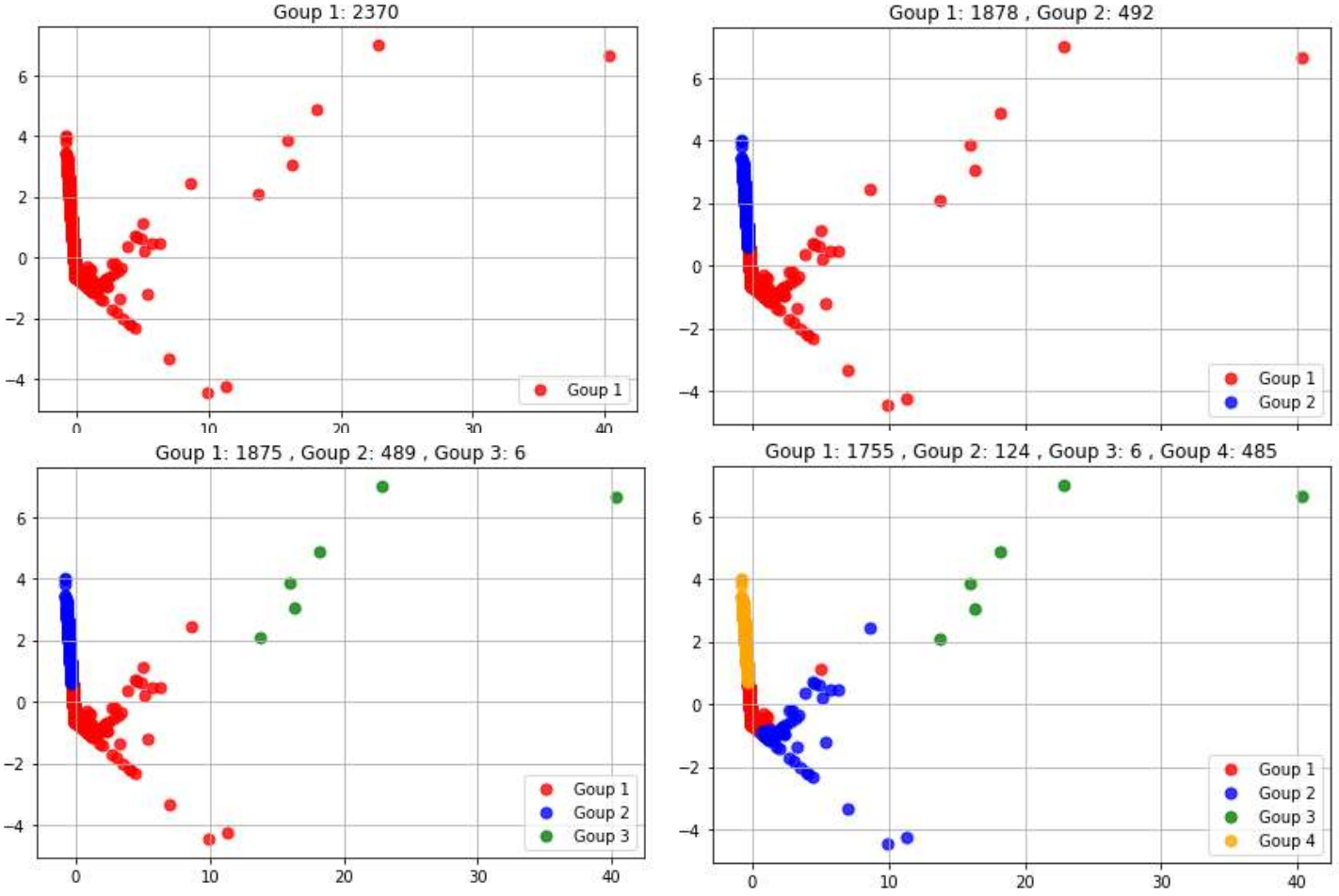
node	da_addr	ipkt	ibyt	flows	pr	flg	dir
1.69.6.1321510	1	2	80	1	1	1	1
1.70.11.1151500	1	1	40	1	1	1	1
10.0.40.2541430	1	1	56	1	1	0	1
10.0.40.2541730	3	1	56	1	1	0	1
10.1.70.2061730	1	3	249	1	1	12	1
10.12.125.100950	3	1	81	1	1	0	1
10.12.125.102240	4	2	92	1	1	0	1
10.42.217.412130	1	13	1144	8	1	0	1
100.26.248.2221210	1	1	40	1	1	1	1
101.32.213.2290550	4	1	40	1	1	1	1
102.134.149.1230250	2	1	40	1	1	1	1
103.100.235.1481450	1	1	52	1	1	1	1
103.101.100.2341750	1	1	40	1	1	1	1
103.118.253.2422210	16	1	44	1	1	1	1
103.139.46.2031750	1	1	52	1	1	1	1
103.146.182.341230	1	1	40	1	1	1	1
103.153.254.1100510	27	1	40	1	1	1	2



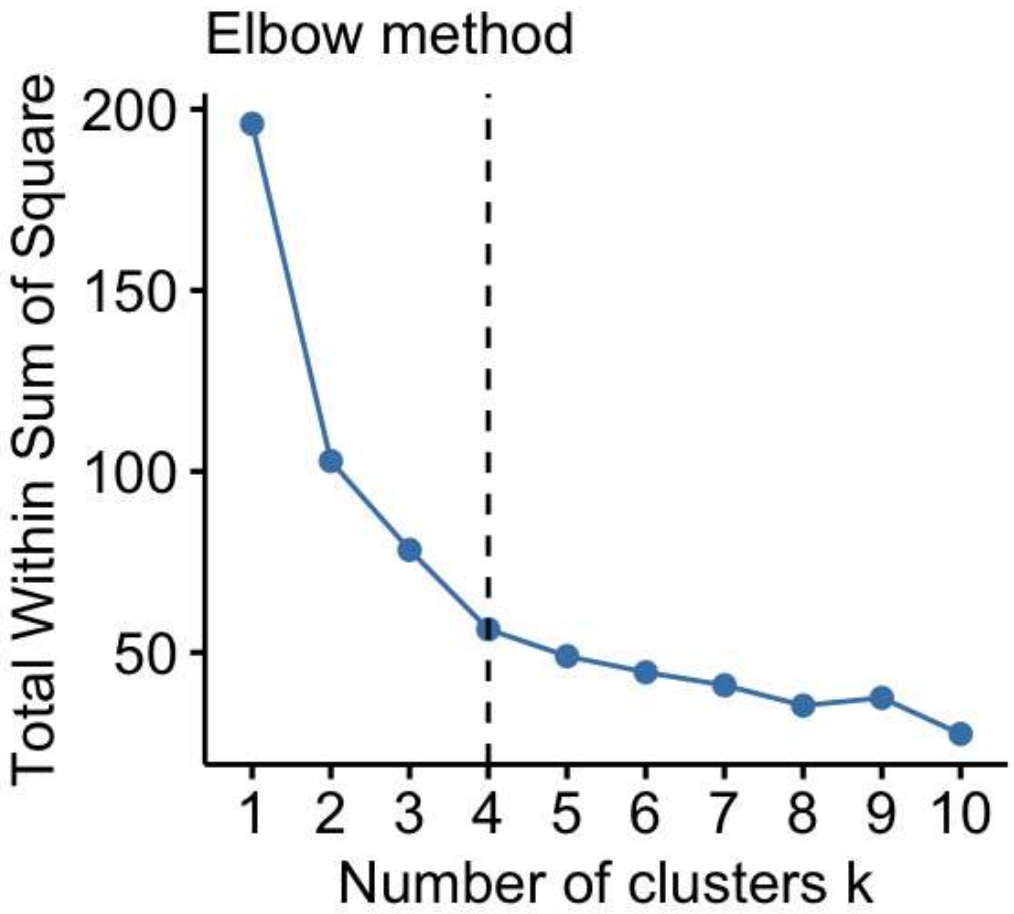


Clustering in hyper-domain (visualization in 3D)

Visualization in 3D

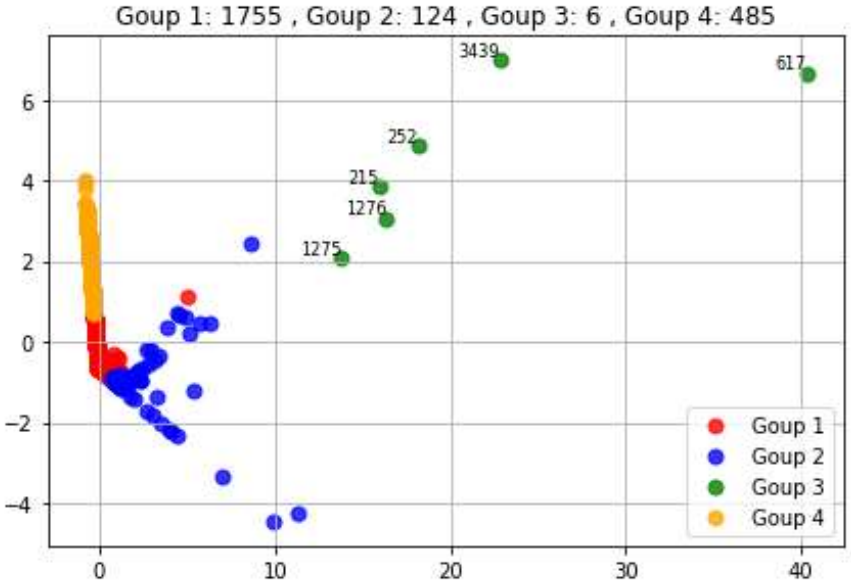


Optimal number of clusters

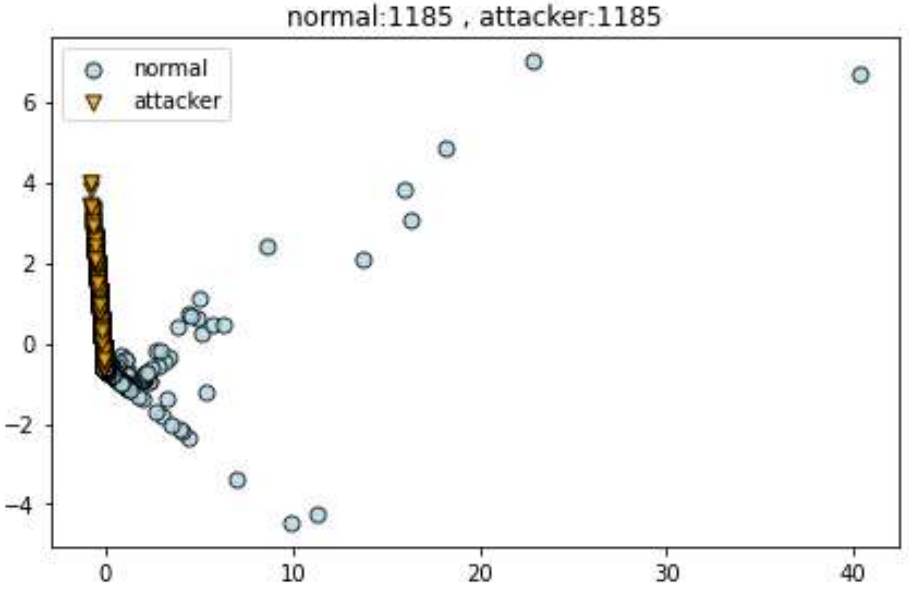


Clustering-Based outlier detection

Clustering results



current rule-based classification result



Group characteristics & Confusion matrix

Group characteristics

Group	mean - da_addr	mean - ipkt	mean - ibyt	mean - flows	Count Group
Group 1	117	19	5779	1	1755
Group 2	2	1302	294637	21	124
Group 3	9	38995	10521734	38	6
Group 4	1248	2	60	1	485
All	342	181	46345	2	2370

Confusion matrix

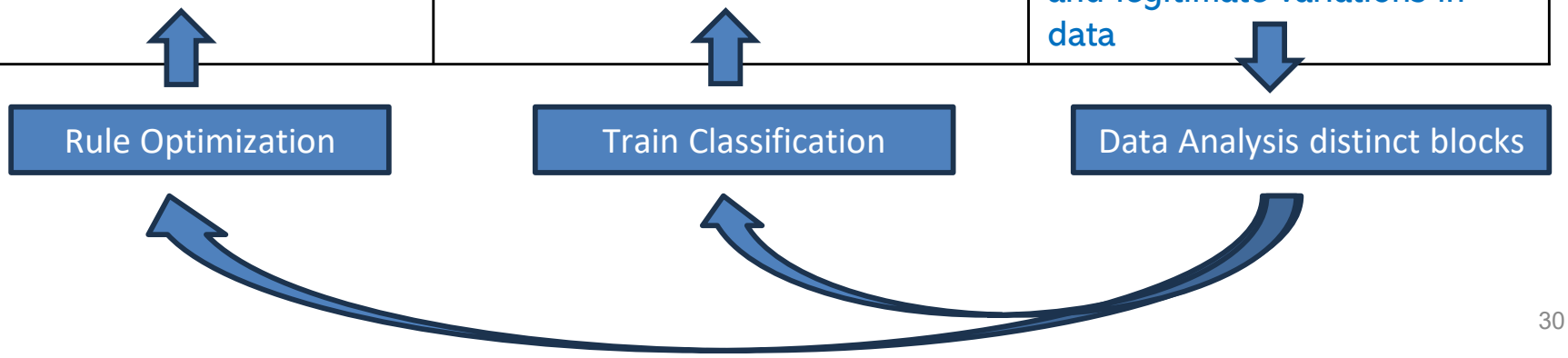
Label	Group 1	Group 2	Group 3	Group 4	Sum
normal	1053	124	6	2	1185
attacker	702			483	1185
Sum	1755	124	6	485	2370

Group	Segment name
Group1	majority 、normal users
Group2	Little high packet 、 traffic users
Group3	Heavy packet 、 traffic users
Group4	high connection count users

Summary & Future Work

- Clustering algorithm provides a different perspective on the classification

Detection Algorithms	Statistical & rule-based decision making	Supervised Learning Classification	Unsupervised Learning Outlier detection
Pros	Transparent and interpretable results	Ability to handle complex relationships	No labels necessary. Useful for finding unusual instances.
Cons	Limited to known rules and assumptions	Requires labeled training data	May have difficulty distinguishing between outliers and legitimate variations in data



NARLabs

Thanks for Your Attention

nfcapd Description

ts	Timestamp	ibyt	Input bytes	nhb	Next hop BGP	mpls6			
te	Time elapsed	opkt	Output packets	svln	Source VLAN	mpls7			
td	Traffic duration	obyt	Output bytes	dvln	Destination VLAN	mpls8			
sa	Source address	in	Input interface	ismc	Input SNMP index	mpls9			
da	Destination address	out	Output interface	odmc	Output SNMP index	mpls10			
sp	Source port	sas	Source AS	idmc	Input destination MAC	cl	Client/server		
dp	Destination port	das	Destination AS	osmc	Output source MAC	sl	Server/client		
pr	Protocol	smk	Source mask	mpls1	MPLS labels 1-10	al	Application layer		
flg	TCP flags	dmk	Destination mask	mpls2		ra	Router/switch IP address		
fwd	Forwarding status	dtos	Destination tos	mpls3		eng	Engine ID		
stos	Source tos	dir	Flow direction	mpls4		exid	Export ID		
ipkt	Input packets	nh	Next hop	mpls5		tr	TCP retransmit coun		