Workshop 2022 | 26 May, 2022

Influence of Features on Accuracy of Anomaly Detection

Senior Researcher, Hoon Ko, Ph.D.

GECAD/ISEP/IPP, hko@isep.ipp.pt

Content

- Introduction
- Related Works
  - Anomaly Signal
  - Energy Network for an Energy Trade Market
- Anomaly Detection Model (ADM)
- Analysis
  - Feature Analysis
  - Correlation of each Feature
- Discussion
- Conclusion

Introduction

Section description

isep Instituto Superior de Engenharia do Porto · gecad · SPET · BeNeFICE · COMPETE · FCT Fundação para a Ciência e a Tecnologia

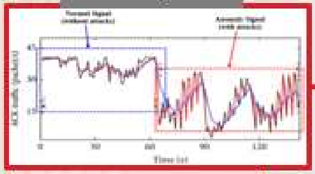
Design a Secure Energy Trading Model based on a Blockchain

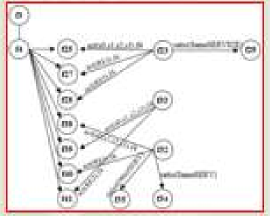
12 January, 2021

By: Hoon Ko, Ph.D, Senior Researcher

- SETM Structure
  - Consists of a multi-Interaction Management Agent (MiM Agent), blockchain and a producer / a consumer.

Data Analysis





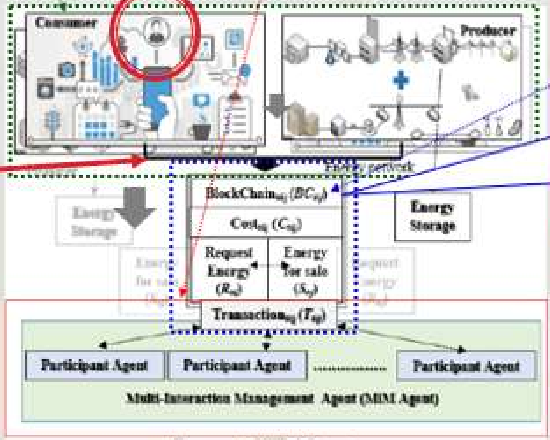

Consumer
Producer
Energy network
Energy Storage
BlockChain$_{sij}$ (BC_{sij})
Cost$_{sij}$ (C_{sij})
Request Energy (R_{sij})
Energy for sale (S_{sij})
Transaction$_{sij}$ (T_{sij})
Energy Storage
Participant Agent
Participant Agent
Participant Agent
Multi-Interaction Management Agent (MIM Agent)

Figure 1. SETM Structure

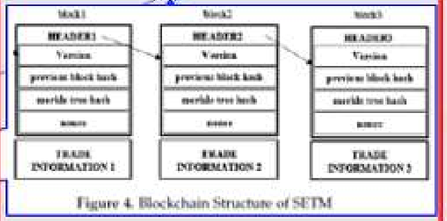
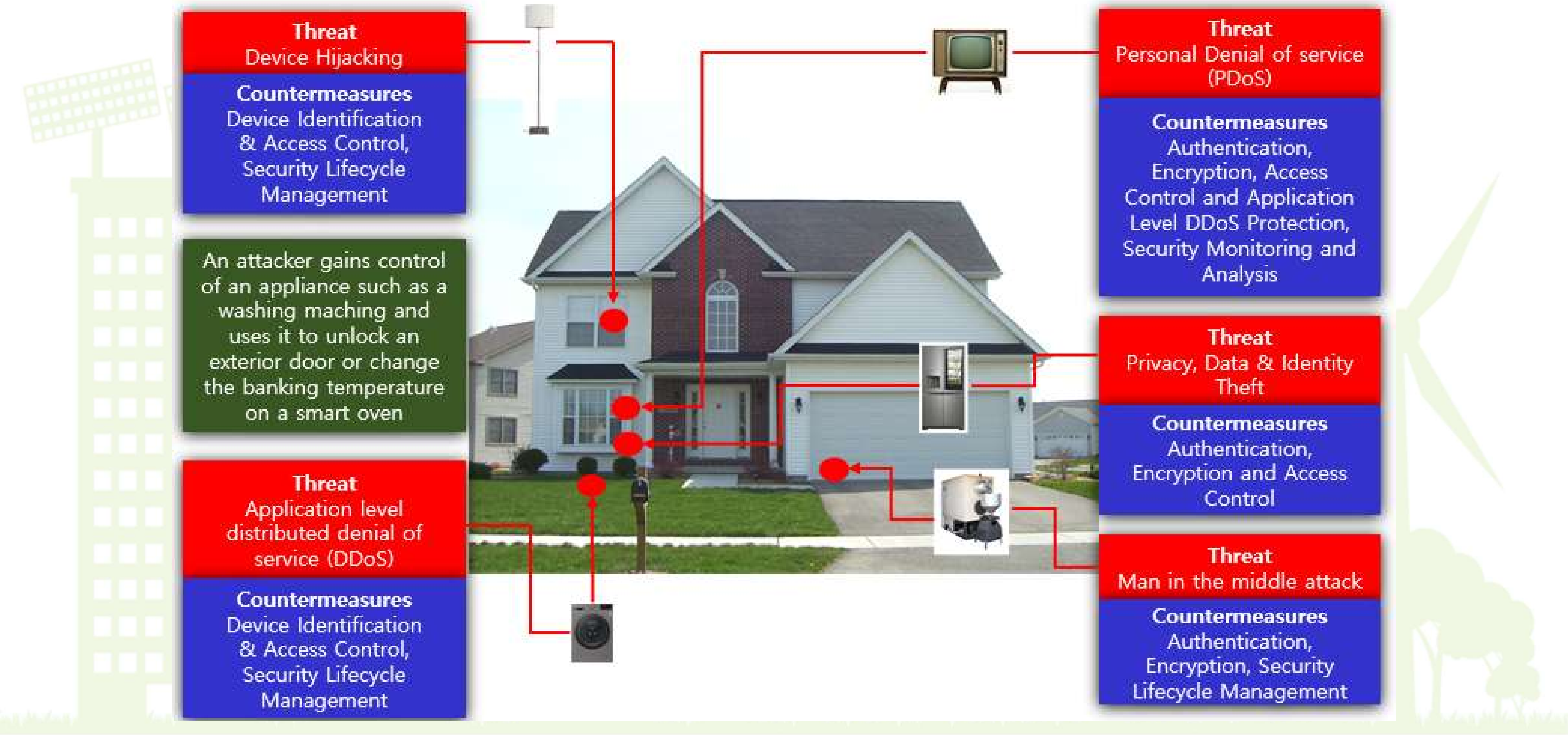


Figure 4. Blockchain Structure of SETM

Feature Correlation

- Networks are prone to cyber attack.(Example)



Threat
Device Hijacking

Countermeasures
Device Identification & Access Control, Security Lifecycle Management

An attacker gains control of an appliance such as a washing maching and uses it to unlock an exterior door or change the banking temperature on a smart oven

Threat
Application level distributed denial of service (DDoS)

Countermeasures
Device Identification & Access Control, Security Lifecycle Management

Threat
Personal Denial of service (PDoS)

Countermeasures
Authentication, Encryption, Access Control and Application Level DDoS Protection, Security Monitoring and Analysis

Threat
Privacy, Data & Identity Theft

Countermeasures
Authentication, Encryption and Access Control

Threat
Man in the middle attack

Countermeasures
Authentication, Encryption, Security Lifecycle Management

Introduction

- **All devices** in a network, such as smart farm, energy system, **can be the targets** by cyber attackers.
  - Smart Farms are using an energy through a farm network for IoT devices.
  - Relevant parties try to trade energy on the energy network by sending each other messages such as reply or request.
  - Now the networks are prone to cyber attack.

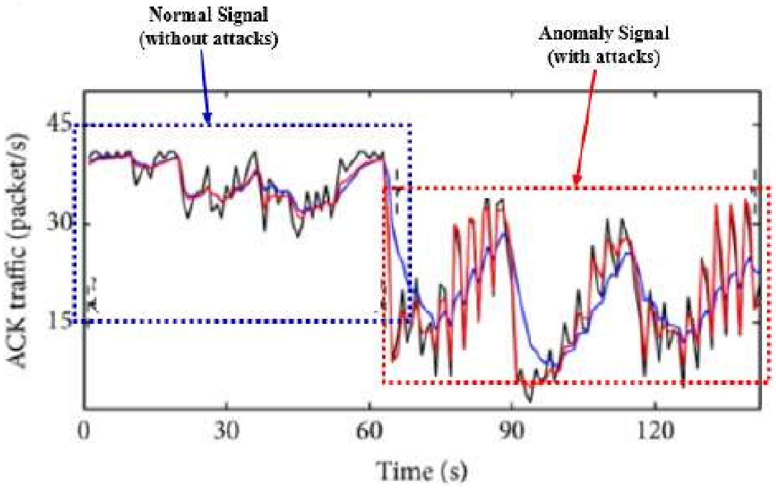
- Need a new security network model for smart places.
  - Strong security qualification in real time detection.
  - (extra) Should detect an anomaly signal by analyzing features correlation.
- Suggesting Model
  - analyzes the anomaly signals of network based on abnormal feature detection
  - (extra) detect by analyzing the relationship between each feature to the anomaly detection model.

Related Works

Section description

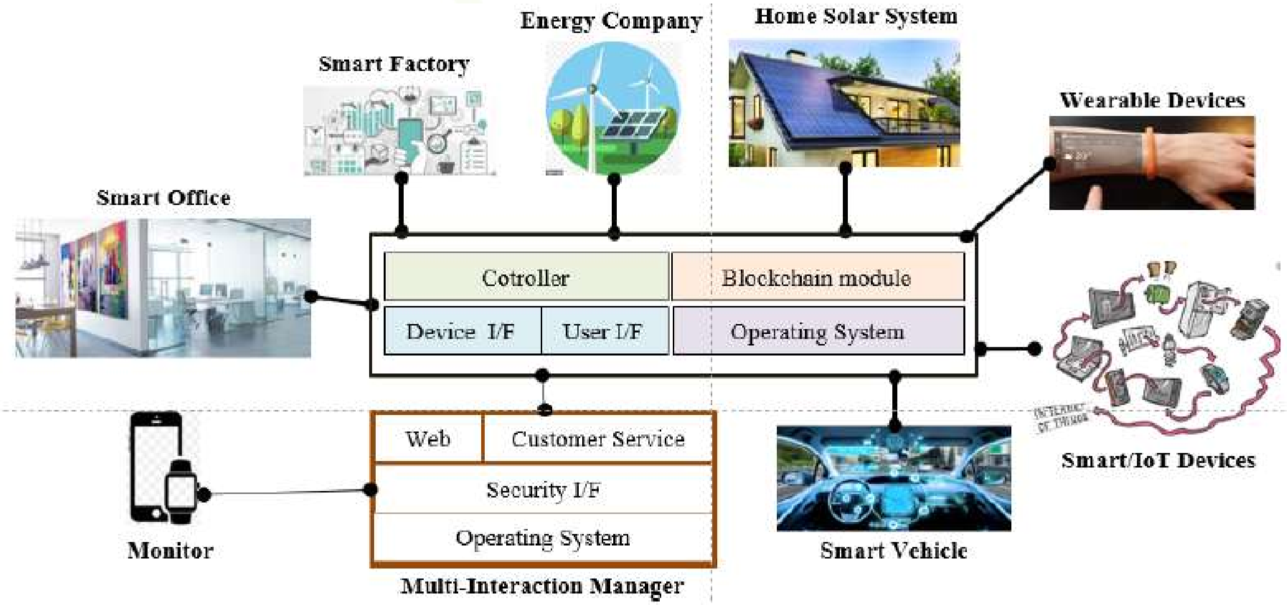
Related Works

- Anomaly Signal
  - When the traffic under attacks is anomaly, the EWMA algorithm smooths the large fluctuation too.
    - While the AEWMA algorithm can retain the anomaly characteristics of the sample value.
  - AEWMA algorithm is more suitable than the EWMA algorithm for DDoS attack detection based on the anomaly characteristics of traffic.



Related Works

- Energy Network for Energy Trade Market
  - The energy generators such as the solar system and the home solar system sending a SHARE message.

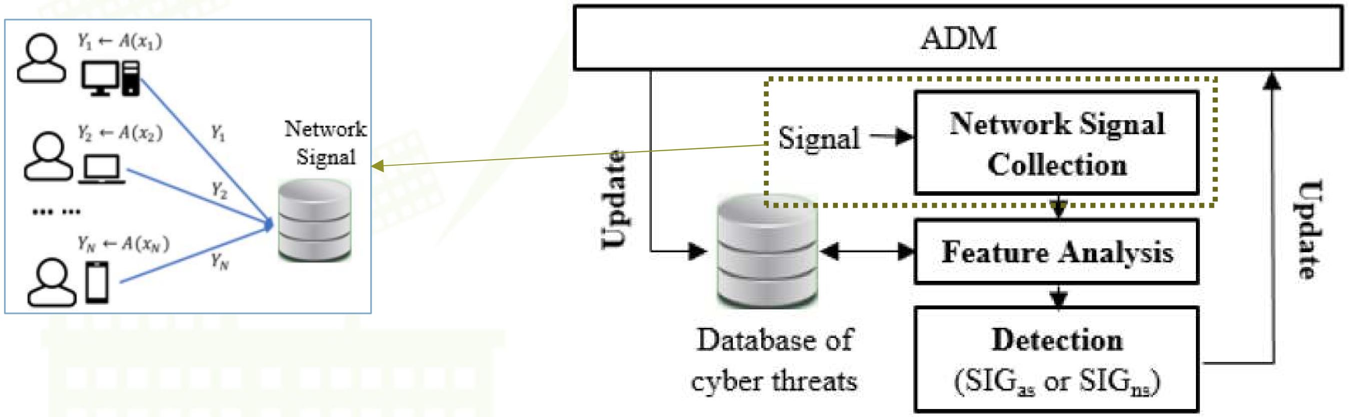


Anomaly Detection Model

Section description

Anomaly Detection Model

- Collection of Network Signals.
  - The ADM consists of the next steps:
    - Network Signal Collection / Feature Analysis / Detection and Update
    - It runs a network signal collection as the first step.
    - In the feature analysis step, it processes by analyzing the relationship of features.



$$Y_i = ADM(X_i) = \begin{cases} 1, with probability = \frac{1}{e^E+1} + \frac{xi}{M} \cdot \frac{e^E-1}{e^E+1} \\ 0, otherwise. \end{cases}$$

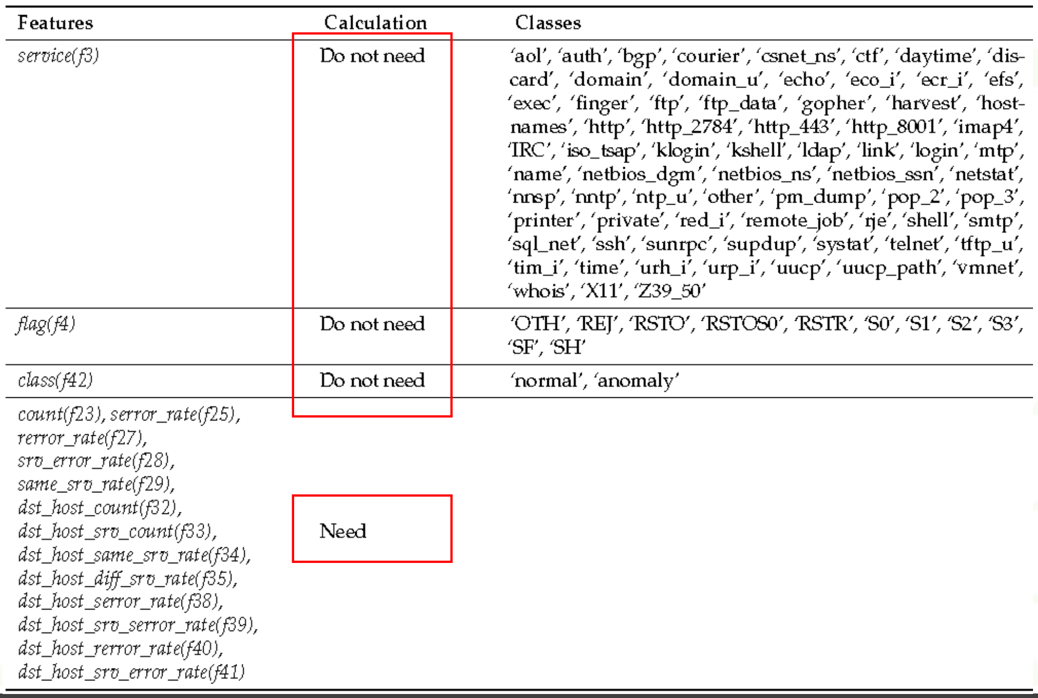
Analysis

Section description

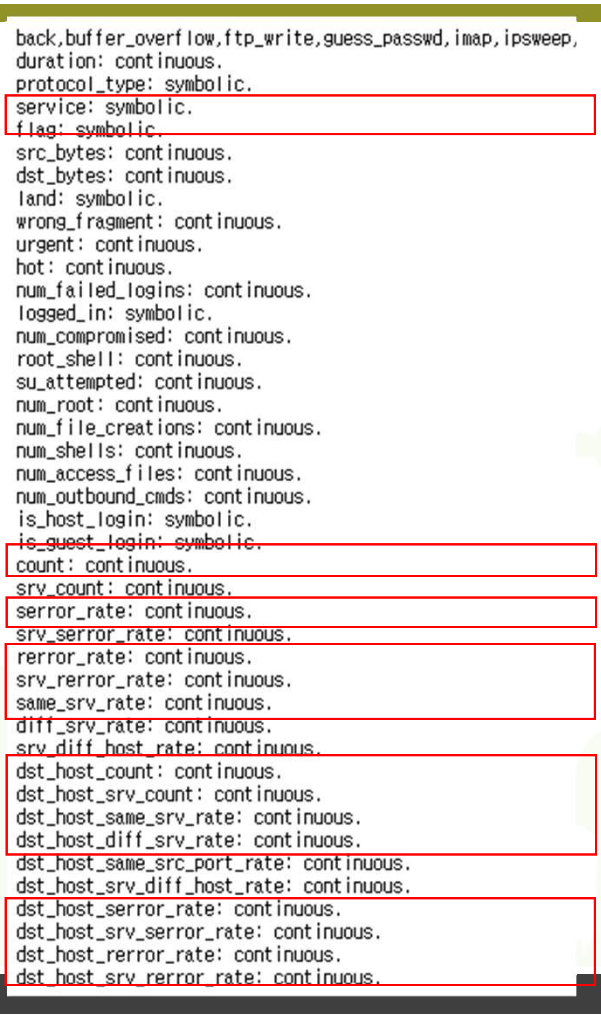
Analysis

- Feature Analysis
  - Tool: WEKA 3.9.5
  - Dataset: KDDCup
    - 42 features / Selected : 15 features + 1 feature (f42)

Table 1. Feature Definition.

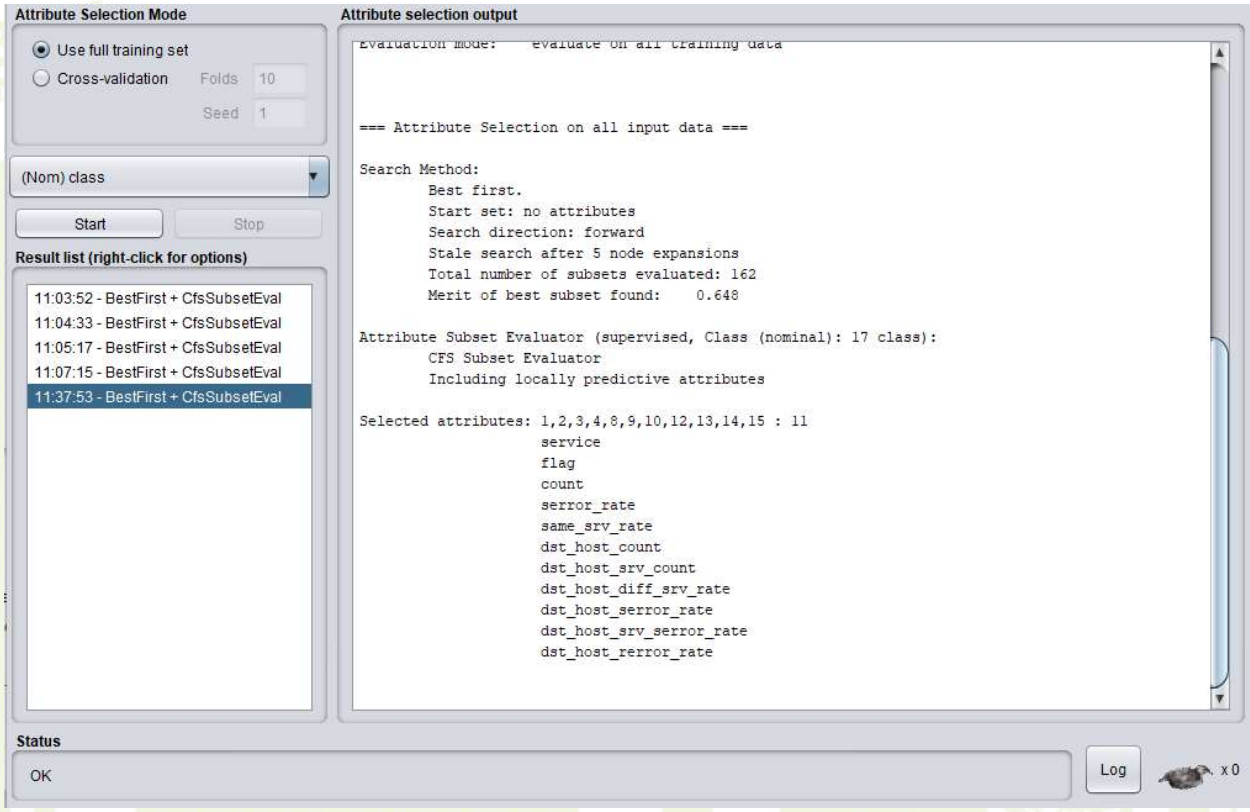


Features	Calculation	Classes
service(f3)	Do not need	'aol', 'auth', 'bgp', 'courier', 'csnet_ns', 'ctf', 'daytime', 'discard', 'domain', 'domain_u', 'echo', 'eco_i', 'ecr_i', 'efs', 'exec', 'finger', 'ftp', 'ftp_data', 'gopher', 'harvest', 'hostnames', 'http', 'http_2784', 'http_443', 'http_8001', 'imap4', 'IRC', 'iso_tsap', 'klogin', 'kshell', 'ldap', 'link', 'login', 'mtp', 'name', 'netbios_dgm', 'netbios_ns', 'netbios_ssn', 'netstat', 'nnsp', 'nntp', 'ntp_u', 'other', 'pm_dump', 'pop_2', 'pop_3', 'printer', 'private', 'red_i', 'remote_job', 'rje', 'shell', 'smtp', 'sql_net', 'ssh', 'sunrpc', 'supdup', 'systat', 'telnet', 'tftp_u', 'tim_i', 'time', 'urh_i', 'urp_i', 'uucp', 'uucp_path', 'vmnet', 'whois', 'X11', 'Z39_50'
flag(f4)	Do not need	'OTH', 'REJ', 'RSTO', 'RSTOS0', 'RSTR', 'S0', 'S1', 'S2', 'S3', 'SF', 'SH'
class(f42)	Do not need	'normal', 'anomaly'
count(f23), serror_rate(f25), rerror_rate(f27), srv_error_rate(f28), same_srv_rate(f29), dst_host_count(f32), dst_host_srv_count(f33), dst_host_same_srv_rate(f34), dst_host_diff_srv_rate(f35), dst_host_serror_rate(f38), dst_host_srv_serror_rate(f39), dst_host_rerror_rate(f40), dst_host_srv_error_rate(f41)	Need	



```
back,buffer_overflow,ftp_write,guess_passwd,imap,ipsweep,
duration: continuous.
protocol_type: symbolic.
service: symbolic.
flag: symbolic.
src_bytes: continuous.
dst_bytes: continuous.
land: symbolic.
wrong_fragment: continuous.
urgent: continuous.
hot: continuous.
num_failed_logins: continuous.
logged_in: symbolic.
num_compromised: continuous.
root_shell: continuous.
su_attempted: continuous.
num_root: continuous.
num_file_creations: continuous.
num_shells: continuous.
num_access_files: continuous.
num_outbound_cmds: continuous.
is_host_login: symbolic.
is_guest_login: symbolic.
count: continuous.
srv_count: continuous.
serror_rate: continuous.
srv_serror_rate: continuous.
rerror_rate: continuous.
srv_rerror_rate: continuous.
same_srv_rate: continuous.
diff_srv_rate: continuous.
srv_diff_host_rate: continuous.
dst_host_count: continuous.
dst_host_srv_count: continuous.
dst_host_same_srv_rate: continuous.
dst_host_diff_srv_rate: continuous.
dst_host_same_src_port_rate: continuous.
dst_host_srv_diff_host_rate: continuous.
dst_host_serror_rate: continuous.
dst_host_srv_serror_rate: continuous.
dst_host_rerror_rate: continuous.
dst_host_srv_rerror_rate: continuous.
```

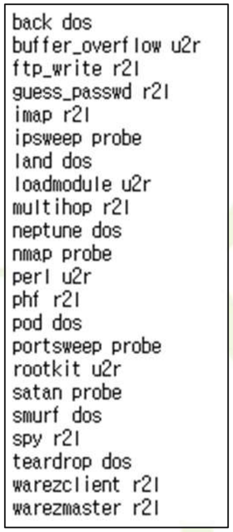
- Case Study: class (f42)
  - normal signal vs anomaly signal



Attribute Selection Mode
● Use full training set
○ Cross-validation
Folds 10
Seed 1
(Nom) class
Start
Stop
Result list (right-click for options)
11:03:52 - BestFirst + CfsSubsetEval
11:04:33 - BestFirst + CfsSubsetEval
11:05:17 - BestFirst + CfsSubsetEval
11:07:15 - BestFirst + CfsSubsetEval
11:37:53 - BestFirst + CfsSubsetEval
Attribute selection output
Status
OK
Log
x 0

```
Evaluation mode:    evaluate on all training data



=== Attribute Selection on all input data ===

Search Method:
        Best first.
        Start set: no attributes
        Search direction: forward
        Stale search after 5 node expansions
        Total number of subsets evaluated: 162
        Merit of best subset found:    0.648

Attribute Subset Evaluator (supervised, Class (nominal): 17 class):
        CFS Subset Evaluator
        Including locally predictive attributes

Selected attributes: 1,2,3,4,8,9,10,12,13,14,15 : 11
                     service
                     flag
                     count
                     serror_rate
                     same_srv_rate
                     dst_host_count
                     dst_host_srv_count
                     dst_host_diff_srv_rate
                     dst_host_serror_rate
                     dst_host_srv_serror_rate
                     dst_host_rerror_rate
```

training_attack_types:
A list of intrusion types.



back	dos
buffer_overflow	u2r
ftp_write	r2l
guess_passwd	r2l
imap	r2l
ipsweep	probe
land	dos
loadmodule	u2r
multihop	r2l
neptune	dos
nmap	probe
perl	u2r
phf	r2l
pod	dos
portsweep	probe
rootkit	u2r
satan	probe
smurf	dos
spy	r2l
teardrop	dos
warezclient	r2l
warezmaster	r2l

Discussion

Section description

Discussion

Table 4. Detailed accuracy by class with a flag.

TP Rate	FP Rate	Precision	Recall	F-Measure	MCC	ROC Area	PRC Area	Class
0.998	0.006	0.996	0.998	0.997	0.992	0.998	0.998	*SF*
0.997	0.003	0.993	0.997	0.995	0.993	0.999	0.998	*S0*
0.987	0.002	0.981	0.987	0.984	0.983	0.996	0.987	*REJ*
0.945	0.001	0.937	0.945	0.941	0.940	0.992	0.917	*RSTR*
0.943	0.000	0.980	0.943	0.962	0.962	0.981	[illegible]	
0.526	0.001	0.674	0.526				[illegible]	
0.272	0.000	0.455	0.272				[illegible]	

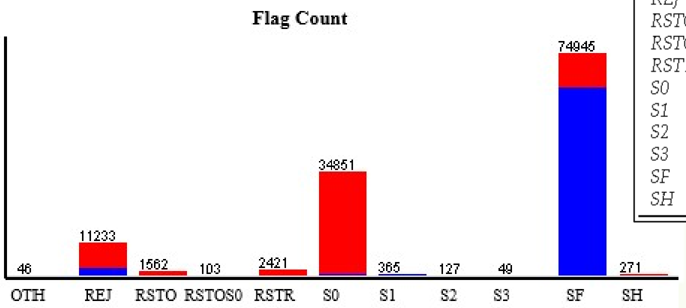


Figure 6. Analysis between service and flag.

Table 5. *flag(f4)* count.

Label	Count
OTH	46
REJ	11,233
RSTO	1562
RSTOS0	103
RSTR	2421
S0	34,851
S1	365
S2	127
S3	49
SF	74,945
SH	271

Table 3. Flag Code.

Code	Description
S0	Connection attempt seen, no reply.
S1	Connection established, not terminated.
SF	Normal establishment and termination. Note that this is the same symbol as for state S1. You can tell the two apart because for S1 there will not be any byte counts in the summary, while for SF there will be.
REJ	Connection attempt rejected.
S2	Connection established and close attempt by originator seen (but no reply from responder).
S3	Connection established and close attempt by responder seen (but no reply from originator).
RSTO	Connection established, originator aborted (sent an RST).
RSTR	Established, responder aborted.
RSTOS0	Originator sent an SYN followed by an RST, we never saw a SYN-ACK from the responder.
RSTRH	Responder sent an SYN ACK followed by an RST, we never saw a SYN from the (purported) originator.
SH	Originator sent an SYN followed by an FIN, we never saw a SYN ACK from the responder (hence the connection was "half" open).
SHR	Responder sent an SYN ACK followed by an FIN, we never saw an SYN from the originator.
OTH	No SYN seen, just midstream traffic (a "partial connection" that was not later closed).

extra

under review

new paper: under review

- Correlation of Each Feature
  - 2 (or 3 including class) features: doesn't need the calculation
  - 13 features: need the calculation

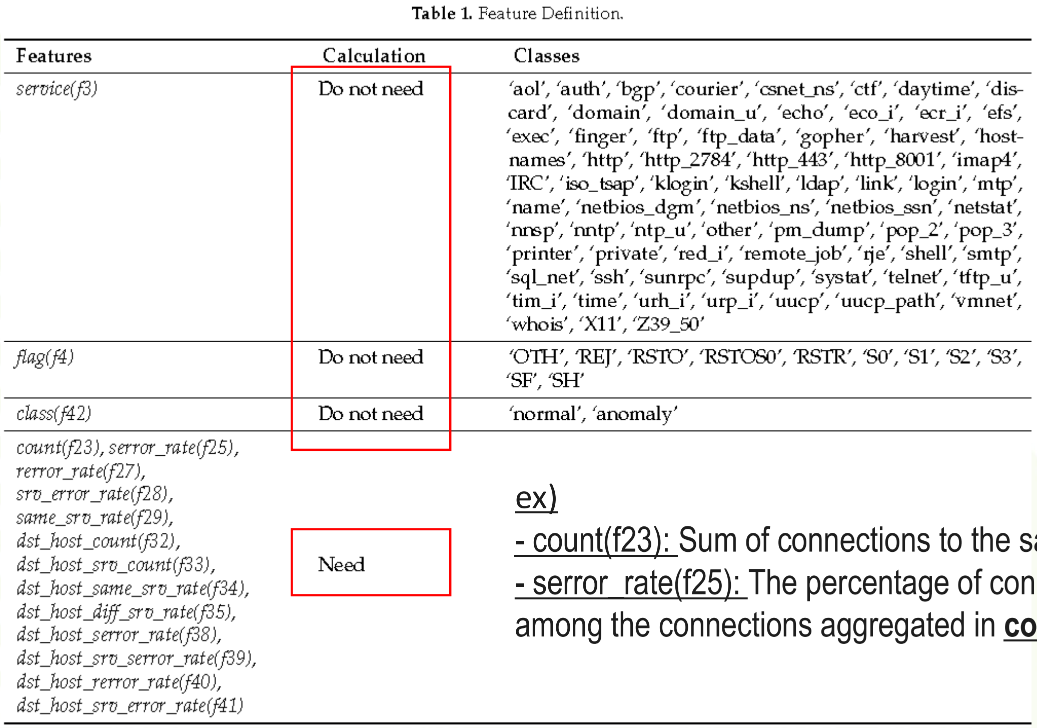


Table 1. Feature Definition.

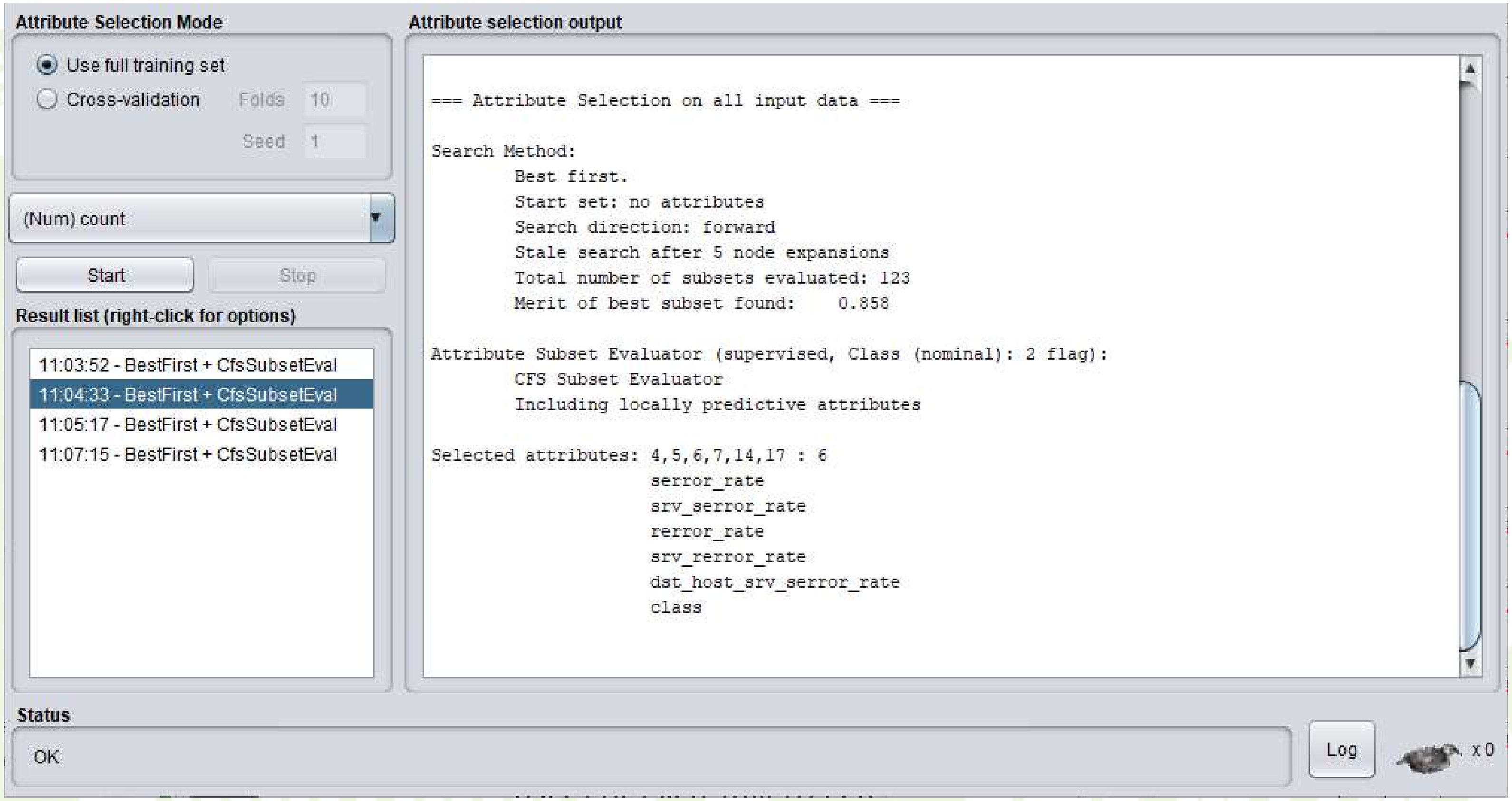
Features	Calculation	Classes
service(f3)	Do not need	'aol', 'auth', 'bgp', 'courier', 'csnet_ns', 'ctf', 'daytime', 'discard', 'domain', 'domain_u', 'echo', 'eco_i', 'ecr_i', 'efs', 'exec', 'finger', 'ftp', 'ftp_data', 'gopher', 'harvest', 'hostnames', 'http', 'http_2784', 'http_443', 'http_8001', 'imap4', 'IRC', 'iso_tsap', 'klogin', 'kshell', 'ldap', 'link', 'login', 'mtp', 'name', 'netbios_dgm', 'netbios_ns', 'netbios_ssn', 'netstat', 'nnsp', 'nntp', 'ntp_u', 'other', 'pm_dump', 'pop_2', 'pop_3', 'printer', 'private', 'red_i', 'remote_job', 'rje', 'shell', 'smtp', 'sql_net', 'ssh', 'sunrpc', 'supdup', 'systat', 'telnet', 'tftp_u', 'tim_i', 'time', 'urh_i', 'urp_i', 'uucp', 'uucp_path', 'vmnet', 'whois', 'X11', 'Z39_50'
flag(f4)	Do not need	'OTH', 'REJ', 'RSTO', 'RSTOS0', 'RSTR', 'S0', 'S1', 'S2', 'S3', 'SF', 'SH'
class(f42)	Do not need	'normal', 'anomaly'
count(f23), serror_rate(f25), rerror_rate(f27), srv_error_rate(f28), same_srv_rate(f29), dst_host_count(f32), dst_host_srv_count(f33), dst_host_same_srv_rate(f34), dst_host_diff_srv_rate(f35), dst_host_serror_rate(f38), dst_host_srv_serror_rate(f39), dst_host_rerror_rate(f40), dst_host_srv_error_rate(f41)	Need	

ex)

- count(f23): Sum of connections to the same destination IP address.

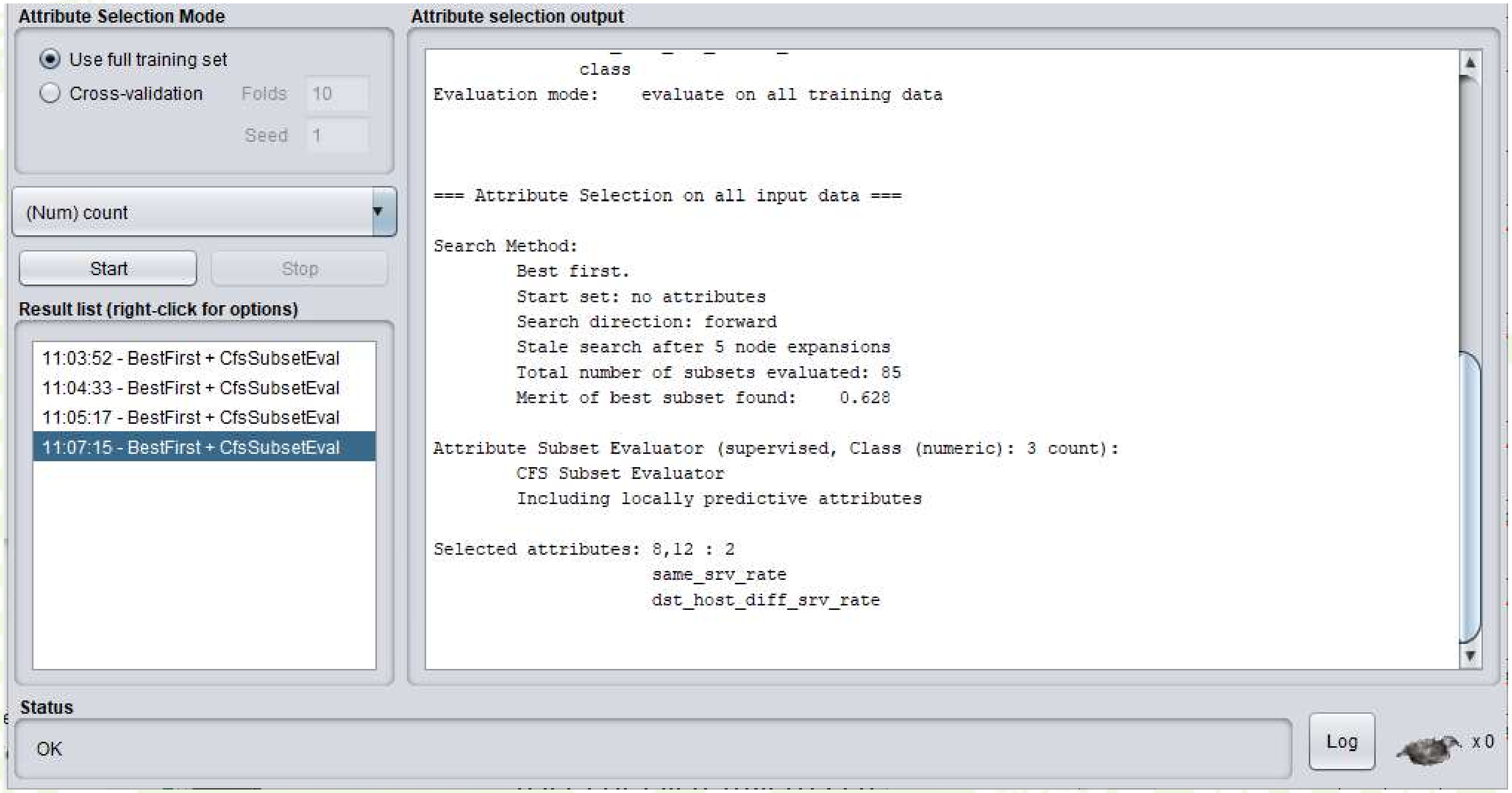
- serror_rate(f25): The percentage of connections that have activated the **flag(f4)** s0, s1, s2 or s3, among the connections aggregated in **count(f23)**.

- Case 2. select ‘f4.flag’ (don’t’need calculation)
  - f4.flag: Connection status: SF, S0, S1, S2, S3, OTH, REJ, RSTO, RSTOS0, SH, RSTRH, SHR.


Attribute Selection Mode
● Use full training set
○ Cross-validation
Folds 10
Seed 1
(Num) count
Start
Stop
Result list (right-click for options)
11:03:52 - BestFirst + CfsSubsetEval
11:04:33 - BestFirst + CfsSubsetEval
11:05:17 - BestFirst + CfsSubsetEval
11:07:15 - BestFirst + CfsSubsetEval
Attribute selection output
Status
OK
Log
x 0

```
=== Attribute Selection on all input data ===

Search Method:
        Best first.
        Start set: no attributes
        Search direction: forward
        Stale search after 5 node expansions
        Total number of subsets evaluated: 123
        Merit of best subset found:    0.858

Attribute Subset Evaluator (supervised, Class (nominal): 2 flag):
        CFS Subset Evaluator
        Including locally predictive attributes

Selected attributes: 4,5,6,7,14,17 : 6
                     serror_rate
                     srv_serror_rate
                     rerror_rate
                     srv_rerror_rate
                     dst_host_srv_serror_rate
                     class
```

- Case 3. select 'f23. count' (calculation)
  - f23.count: Sum of connections to the same destination IP address.



Attribute Selection Mode

● Use full training set

○ Cross-validation Folds 10

Seed 1

(Num) count

Result list (right-click for options)

- 11:03:52 - BestFirst + CfsSubsetEval
- 11:04:33 - BestFirst + CfsSubsetEval
- 11:05:17 - BestFirst + CfsSubsetEval
- 11:07:15 - BestFirst + CfsSubsetEval

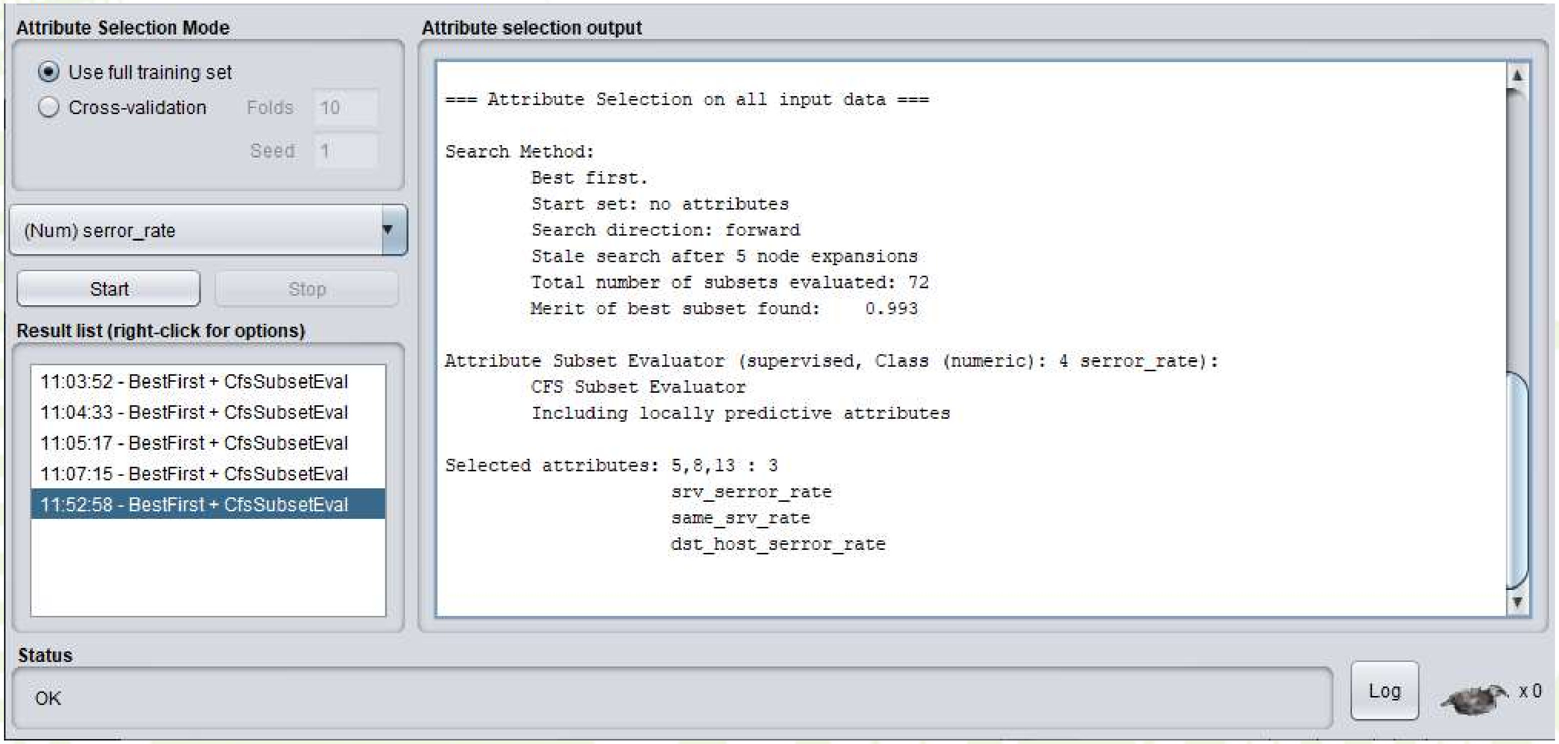
Attribute selection output

```
              class
Evaluation mode:    evaluate on all training data



=== Attribute Selection on all input data ===

Search Method:
        Best first.
        Start set: no attributes
        Search direction: forward
        Stale search after 5 node expansions
        Total number of subsets evaluated: 85
        Merit of best subset found:    0.628

Attribute Subset Evaluator (supervised, Class (numeric): 3 count):
        CFS Subset Evaluator
        Including locally predictive attributes

Selected attributes: 8,12 : 2
                     same_srv_rate
                     dst_host_diff_srv_rate
```

Status

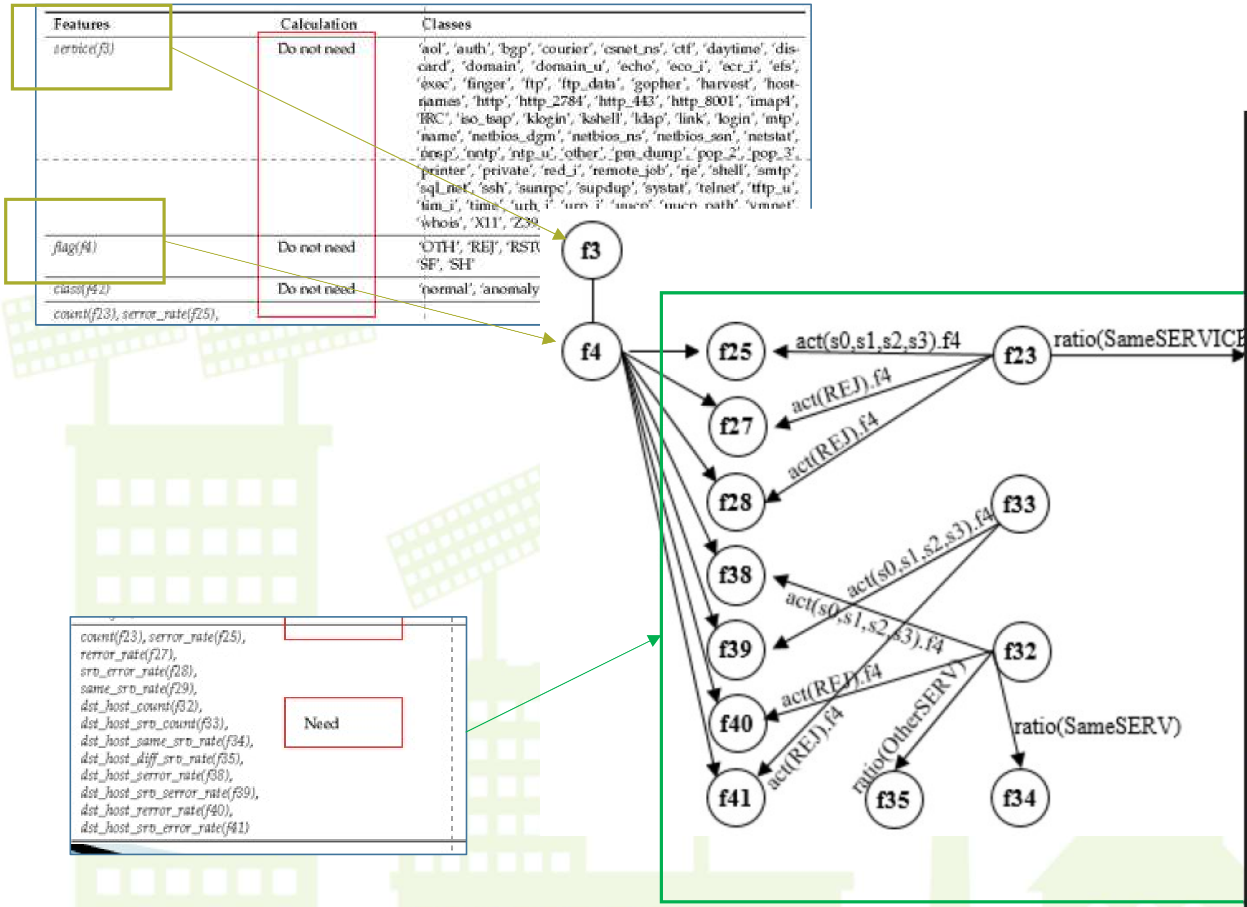
OK

- Case 5. select ‘25.serror_rate’ (calculation)
    - f25.serror_rate: The percentage of connections that have activated the flag(f4) s0, s1, s2 or s3, among the connections aggregated in count(f23).

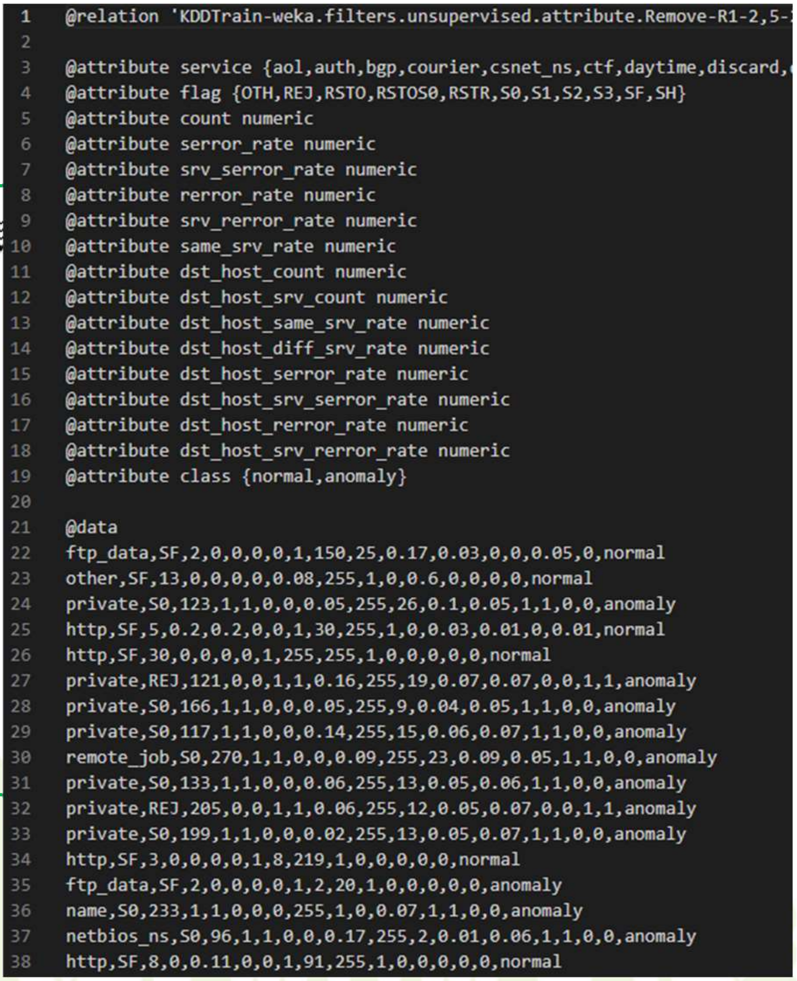


Attribute Selection Mode
● Use full training set
○ Cross-validation
Folds
10
Seed
1
(Num) serror_rate
Start
Stop
Result list (right-click for options)
11:03:52 - BestFirst + CfsSubsetEval
11:04:33 - BestFirst + CfsSubsetEval
11:05:17 - BestFirst + CfsSubsetEval
11:07:15 - BestFirst + CfsSubsetEval
11:52:58 - BestFirst + CfsSubsetEval
Attribute selection output
Status
OK
Log
x 0

```
=== Attribute Selection on all input data ===

Search Method:
        Best first.
        Start set: no attributes
        Search direction: forward
        Stale search after 5 node expansions
        Total number of subsets evaluated: 72
        Merit of best subset found:    0.993

Attribute Subset Evaluator (supervised, Class (numeric): 4 serror_rate):
        CFS Subset Evaluator
        Including locally predictive attributes

Selected attributes: 5,8,13 : 3
                     srv_serror_rate
                     same_srv_rate
                     dst_host_serror_rate
```



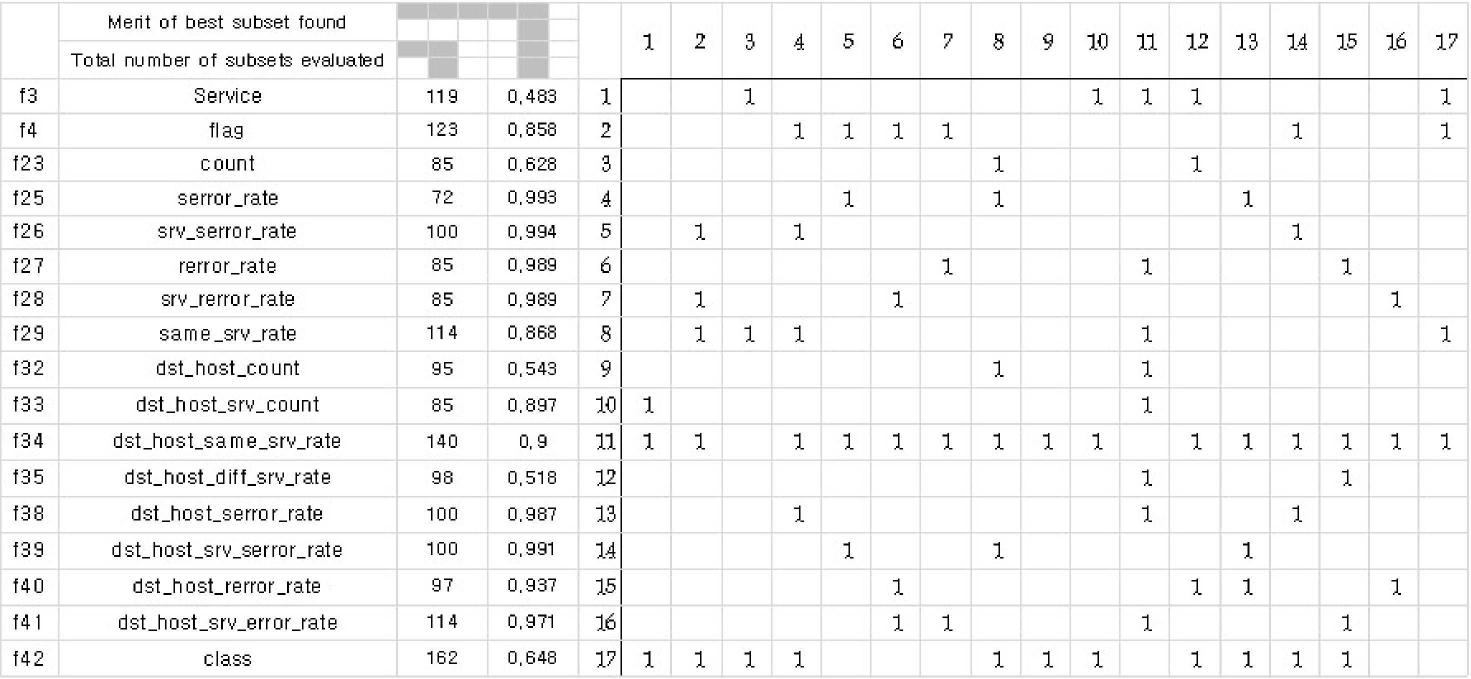
Features	Calculation	Classes
service(f3)	Do not need	'aol', 'auth', 'bgp', 'courier', 'csnet_ns', 'ctf', 'daytime', 'discard', 'domain', 'domain_u', 'echo', 'eco_i', 'ecr_i', 'efs', 'exec', 'finger', 'ftp', 'ftp_data', 'gopher', 'harvest', 'hostnames', 'http', 'http_2784', 'http_443', 'http_8001', 'imap4', 'IRC', 'iso_tsap', 'klogin', 'kshell', 'ldap', 'link', 'login', 'mtp', 'name', 'netbios_dgm', 'netbios_ns', 'netbios_ssn', 'netstat', 'nnsp', 'nntp', 'ntp_u', 'other', 'pm_dump', 'pop_2', 'pop_3', 'printer', 'private', 'red_i', 'remote_job', 'rje', 'shell', 'smtp', 'sql_net', 'ssh', 'sunrpc', 'supdup', 'systat', 'telnet', 'tftp_u', 'tim_i', 'time', 'urh_i', 'urp_i', 'uucp', 'uucp_path', 'vmnet', 'whois', 'X11', 'Z39
flag(f4)	Do not need	'OTH', 'REJ', 'RST 'SF', 'SH'
class(f42)	Do not need	'normal', 'anomaly
count(f23), serror_rate(f25), *rerror_rate(f27),* *srv_error_rate(f28),* *same_srv_rate(f29),* *dst_host_count(f32),* *dst_host_srv_count(f33),* *dst_host_same_srv_rate(f34),* *dst_host_diff_srv_rate(f35),* *dst_host_serror_rate(f38),* *dst_host_srv_serror_rate(f39),* *dst_host_rerror_rate(f40),* *dst_host_srv_error_rate(f41)*	Need	



```
@relation 'KDDTrain-weka.filters.unsupervised.attribute.Remove-R1-2,5-

@attribute service {aol,auth,bgp,courier,csnet_ns,ctf,daytime,discard,
@attribute flag {OTH,REJ,RSTO,RSTOS0,RSTR,S0,S1,S2,S3,SF,SH}
@attribute count numeric
@attribute serror_rate numeric
@attribute srv_serror_rate numeric
@attribute rerror_rate numeric
@attribute srv_rerror_rate numeric
@attribute same_srv_rate numeric
@attribute dst_host_count numeric
@attribute dst_host_srv_count numeric
@attribute dst_host_same_srv_rate numeric
@attribute dst_host_diff_srv_rate numeric
@attribute dst_host_serror_rate numeric
@attribute dst_host_srv_serror_rate numeric
@attribute dst_host_rerror_rate numeric
@attribute dst_host_srv_rerror_rate numeric
@attribute class {normal,anomaly}

@data
ftp_data,SF,2,0,0,0,0,1,150,25,0.17,0.03,0,0,0.05,0,normal
other,SF,13,0,0,0,0,0.08,255,1,0,0.6,0,0,0,0,normal
private,S0,123,1,1,0,0,0.05,255,26,0.1,0.05,1,1,0,0,anomaly
http,SF,5,0.2,0.2,0,0,1,30,255,1,0,0.03,0.01,0,0.01,normal
http,SF,30,0,0,0,0,1,255,255,1,0,0,0,0,0,normal
private,REJ,121,0,0,1,1,0.16,255,19,0.07,0.07,0,0,1,1,anomaly
private,S0,166,1,1,0,0,0.05,255,9,0.04,0.05,1,1,0,0,anomaly
private,S0,117,1,1,0,0,0.14,255,15,0.06,0.07,1,1,0,0,anomaly
remote_job,S0,270,1,1,0,0,0.09,255,23,0.09,0.05,1,1,0,0,anomaly
private,S0,133,1,1,0,0,0.06,255,13,0.05,0.06,1,1,0,0,anomaly
private,REJ,205,0,0,1,1,0.06,255,12,0.05,0.07,0,0,1,1,anomaly
private,S0,199,1,1,0,0,0.02,255,13,0.05,0.07,1,1,0,0,anomaly
http,SF,3,0,0,0,0,1,8,219,1,0,0,0,0,0,normal
ftp_data,SF,2,0,0,0,0,1,2,20,1,0,0,0,0,0,anomaly
name,S0,233,1,1,0,0,0,255,1,0,0.07,1,1,0,0,anomaly
netbios_ns,S0,96,1,1,0,0,0.17,255,2,0.01,0.06,1,1,0,0,anomaly
http,SF,8,0,0.11,0,0,1,91,255,1,0,0,0,0,0,normal
```

- Done all features with ‘select attributes’
  - Can be dataset as an input in GNN (Graph Neural Networks)

※ KDDCup10+17-DDoS.arff



	Merit of best subset found				1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
	Total number of subsets evaluated																				
f3	Service	119	0.483	1			1							1	1	1					1
f4	flag	123	0.858	2				1	1	1	1							1			1
f23	count	85	0.628	3								1				1					
f25	serror_rate	72	0.993	4					1			1					1				
f26	srv_serror_rate	100	0.994	5		1		1										1			
f27	rerror_rate	85	0.989	6							1				1				1		
f28	srv_rerror_rate	85	0.989	7		1				1										1	
f29	same_srv_rate	114	0.868	8		1	1	1							1						1
f32	dst_host_count	95	0.543	9								1			1						
f33	dst_host_srv_count	85	0.897	10	1										1						
f34	dst_host_same_srv_rate	140	0.9	11	1	1		1	1	1	1	1	1	1		1	1	1	1	1	1
f35	dst_host_diff_srv_rate	98	0.518	12											1				1		
f38	dst_host_serror_rate	100	0.987	13				1							1			1			
f39	dst_host_srv_serror_rate	100	0.991	14					1			1					1				
f40	dst_host_rerror_rate	97	0.937	15						1						1	1			1	
f41	dst_host_srv_error_rate	114	0.971	16						1	1				1				1		
f42	class	162	0.648	17	1	1	1	1				1	1	1		1	1	1	1		

- Flow of the GNN

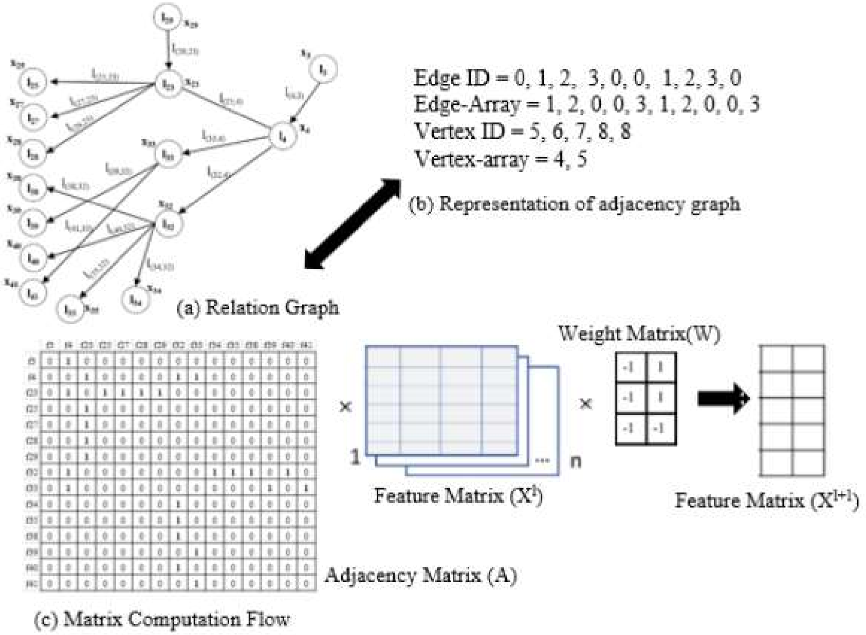

Edge ID = 0, 1, 2, 3, 0, 0, 1, 2, 3, 0
Edge-Array = 1, 2, 0, 0, 3, 1, 2, 0, 0, 3
Vertex ID = 5, 6, 7, 8, 8
Vertex-array = 4, 5
(b) Representation of adjacency graph
(a) Relation Graph
Weight Matrix(W)
Feature Matrix (X^l)
Feature Matrix (X^{l+1})
Adjacency Matrix (A)
(c) Matrix Computation Flow

Fig. 1 Flow of GNN

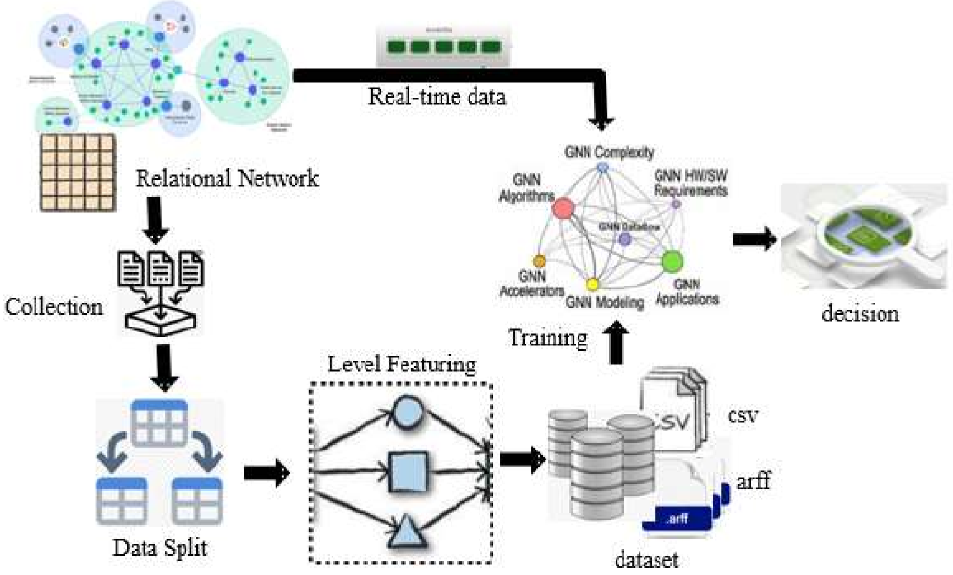


Fig. 2 Methodology

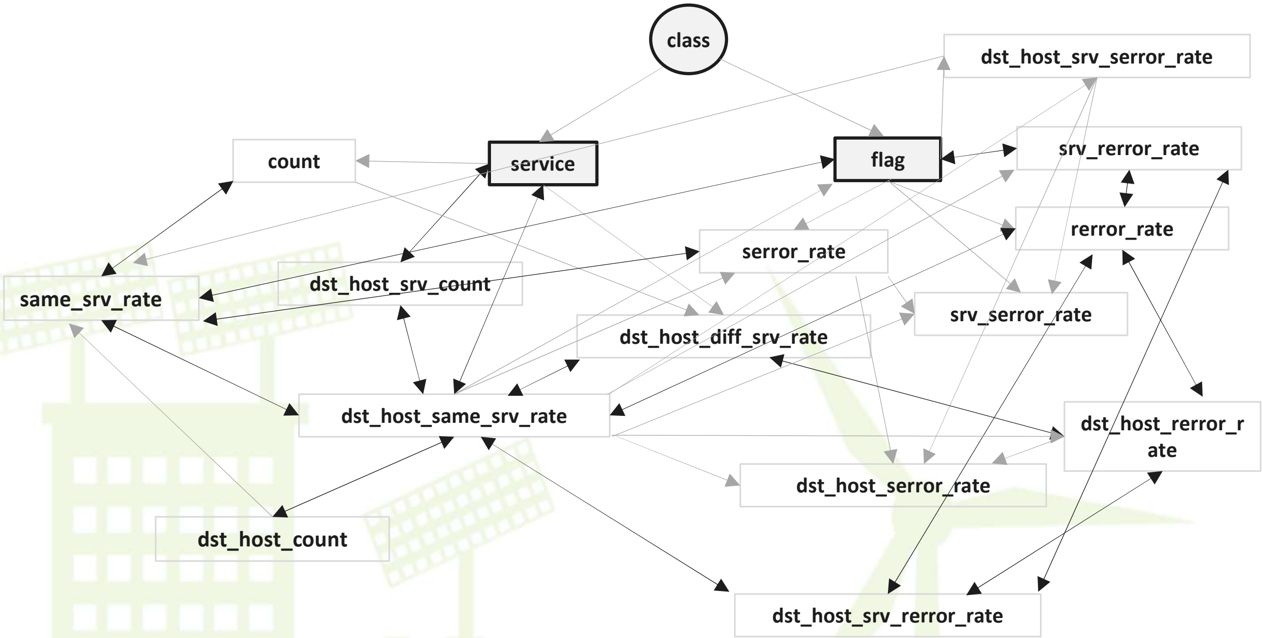


Table 6 Correct Instances of KDDCup

Based Feature	Type	Correct State	Accuracy
service	Correctly Classifier Instances	90522	71.8583
	Incorrectly Classified Instances	35451	28.1417
	Kappa statistic	0.6567	
	Mean absolute error (MAE)	0.0108	
	Root mean squared error (RMSE)	0.0756	
flag	Correctly Classifier Instances	124520	98.8466
	Incorrectly Classified Instances	1453	1.1534
	Kappa statistic	0.9794	
	Mean absolute error (MAE)	0.0032	
	Root mean squared error (RMSE)	0.0424	

Conclusion

- We have conducted an accuracy analysis based on the feature.
  - The problem with the existing methods has been that real-time processing of the anomaly signal discovery is challenging.

- To solve this, we proposed an update of the anomaly signal, focused around the features, and a method to detect the anomaly signal based on the selected features.

- In this study (in the algorithm), the features that can be selected from raw data were service(f3) and flag(f4).
  - The flag(f4) was selected over service(f3) for its relatively higher accuracy score.

- In the results, it determined the anomaly with 99.7% (0.997) accuracy in f(4)(S0), and in case f(4)(REJ) received 11,233 signals with a normal or 171 anomaly judgment accuracy of 98.7% (0.987).

isep Instituto Superior de Engenharia do Porto
gecad
P.PORTO
SPET
BeNeFICE
FCT Fundação para a Ciência e a Tecnologia
PORTUGAL 2020
UNIÃO EUROPEIA Fundo Europeu de Desenvolvimento Regional

Questions ...

Thank You ...