



ESPE

UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA



SEDE
SANTO DOMINGO

UNIVERSIDAD DE LAS FUERZAS ARMADAS - ESPE

Trabajo de titulación, previo a la obtención del título de Ingeniería en
Tecnologías de la Información

“Clasificación de ataques mediante técnicas de aprendizaje automático en Redes Definidas por Software ”

Autor: Castillo Camacho, Miguel Angel

Tutor: Msc. Nuñez Agurto, Alberto Daniel Mgtr.

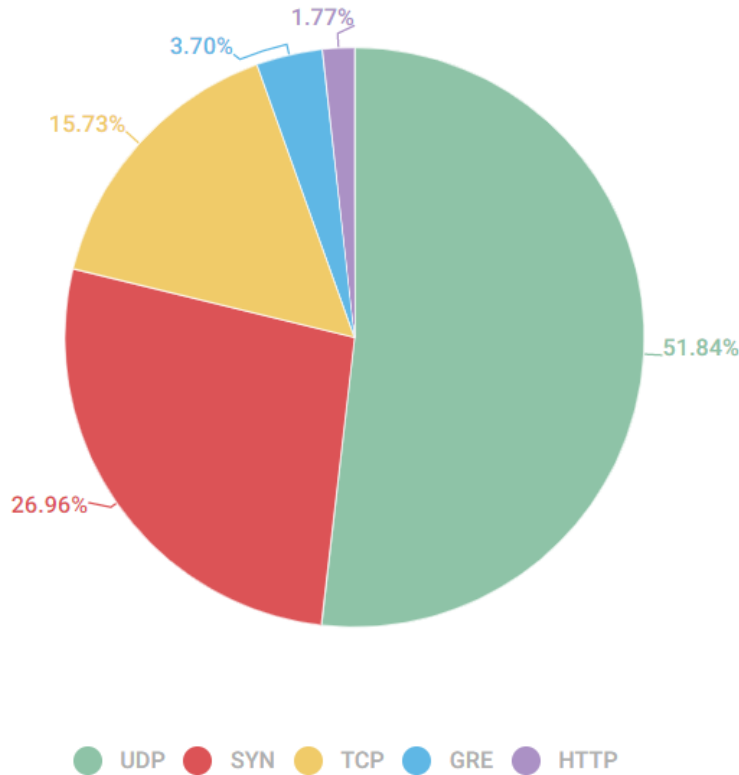


Agenda

- Introducción
- Problemática
- Objetivos
- Marco Conceptual
- Revisión Sistemática de la Literatura
- Propuesta de solución
- Metodología
- Desarrollo
- Implementación
- Resultados
- Conclusiones
- Recomendaciones
- Trabajos Futuros

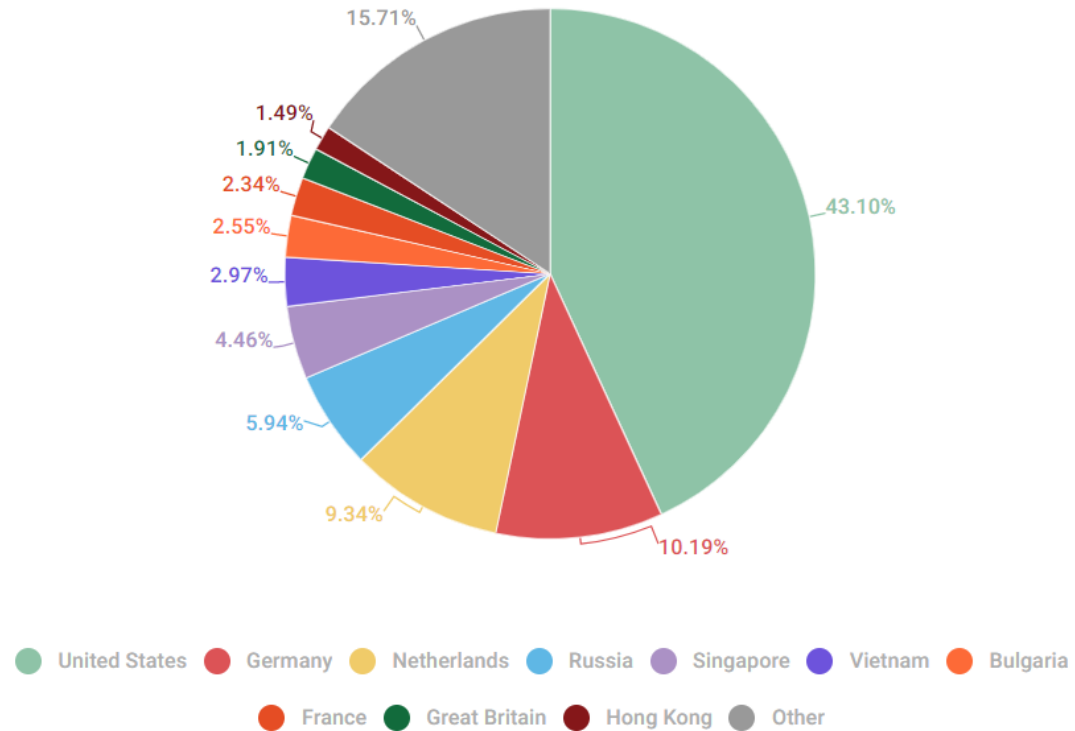
Introducción

Distribución de ataques DDoS.



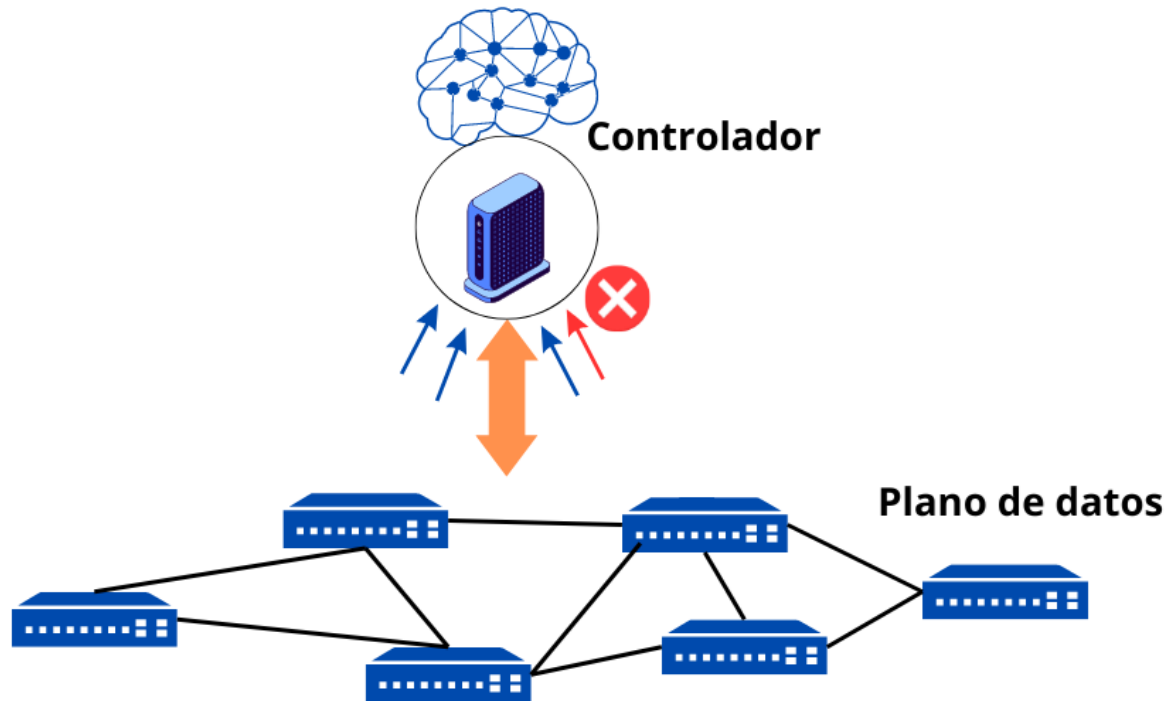
Recuperado de Kaspersky (2022).

Ataques dirigidos a infraestructuras de redes llevados a cabo por Botnets.



Problemática

- SDN presenta amenazas más graves que las redes tradicionales debido a las vulnerabilidades que presenta un componente centralizado de control.



Objetivos

Objetivo General

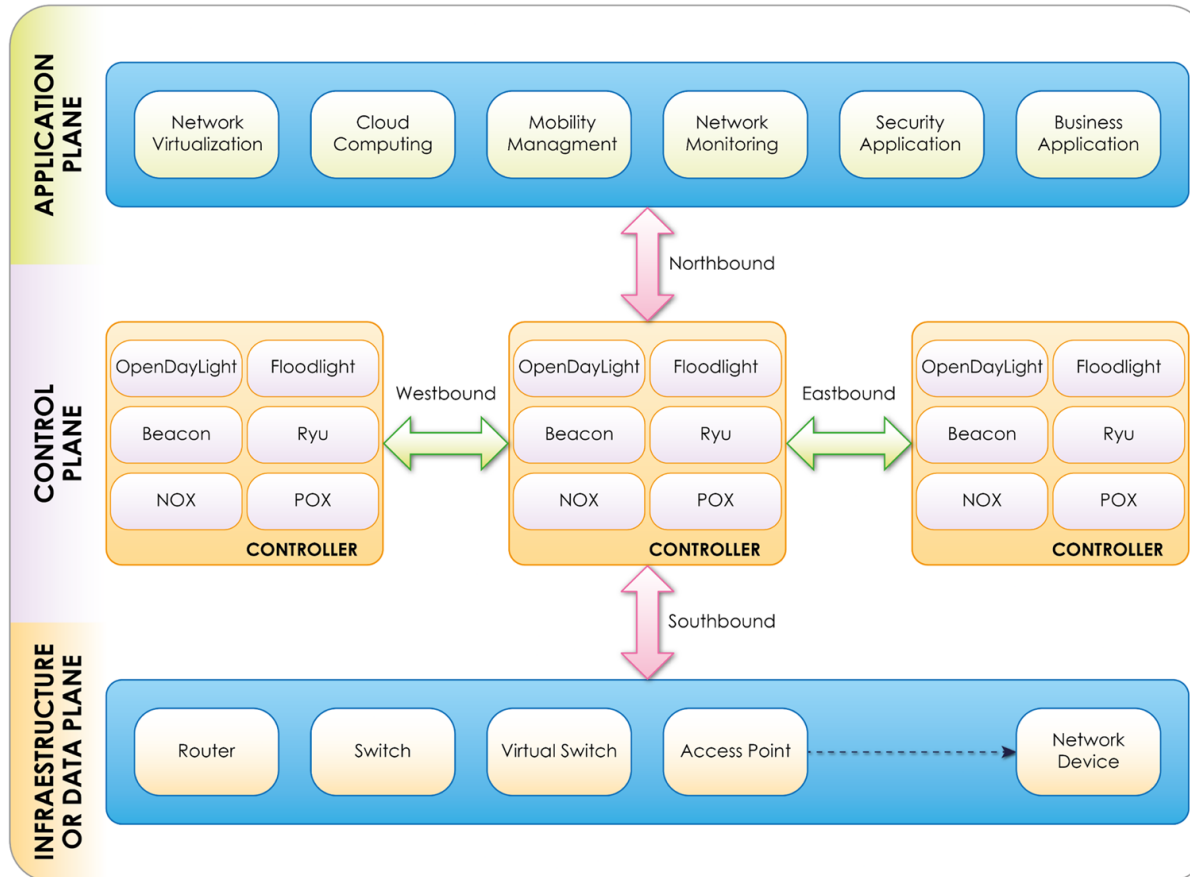
Definir un modelo de clasificación de ataques mediante el uso de técnicas de aprendizaje automático en Redes Definidas por Software.

Objetivos Específicos

- ❖ Determinar los enfoques de clasificación de ataques y los trabajos relacionados en el ámbito de seguridad en SDN.
- ❖ Realizar la selección de algoritmos de aprendizaje automático y el conjunto de datos apropiado para entrenar el modelo de clasificación de ataques en SDN.
- ❖ Desarrollar la implementación del modelo de clasificación de ataques en un escenario emulado.
- ❖ Evaluar el modelo de clasificación de ataques.

Marco Conceptual

Arquitectura de Red Definida por Software



Recuperado de Núñez (2022).

Marco Conceptual

Controladores open source

CONTROLADOR	LENGUAJE DE PROGRAMACIÓN	PLATAFORMA
NOX	C++	LINUX
POX	PYTHON	LINUX, MAC OS Y WINDOWS
FLOODLIGHT	JAVA	LINUX, MAC OS Y WINDOWS
OPENDAYLIGHT	JAVA	LINUX, MAC OS Y WINDOWS
RYU	PYTHON	LINUX
TREMA	RUBY Y C	LINUX
ONOS	JAVA	LINUX, MAC OS Y WINDOWS
BEACON	JAVA	LINUX, MAC OS Y WINDOWS



Marco Conceptual

Métodos de clasificación de tráfico

1. Analizar los paquetes activos de la red y clasificarlos según el puerto de las aplicaciones



```
232 12.000044 192.168.1.129 192.168.1.149 TLSv1.2 86 Application Data
250 13.281844 192.168.1.149 ec2-52-22-91-10.compute-1.amazonaws.com TLSv1.2 92 Application Data
251 13.383613 ec2-52-22-91-10.compute-1.amazonaws.com 192.168.1.149 TLSv1.2 86 Application Data
357 20.308904 192.168.1.149 protegermpc.net TLSv1.2 212 Client Hello
359 20.815100 protegermpc.net 192.168.1.149 TLSv1.2 1514 Server Hello
361 20.815101 protegermpc.net 192.168.1.149 TLSv1.2 1230 Certificate (TCP segment of a
362 20.815102 protegermpc.net 192.168.1.149 TLSv1.2 115 Server Key Exchange, Server Hel
364 20.81714 192.168.1.149 protegermpc.net TLSv1.2 347 Client Key Exchange, Change Cip
365 20.825802 protegermpc.net 192.168.1.149 TLSv1.2 328 New Session Ticket, Change Cliph
375 21.077524 192.168.1.149 ec2-18-195-87-124.eu-central-1.compu... TLSv1.2 463 Application Data
376 21.077607 192.168.1.149 protegermpc.net TLSv1.2 423 Application Data
380 21.150864 192.168.1.149 ec2-18-195-87-124.eu-central-1.compu... TLSv1.2 318 Application Data
382 21.183205 ec2-18-195-87-124.eu-central-1.compu... 192.168.1.149 TLSv1.2 348 Application Data
```

> Frame 376: 623 bytes on wire (4984 bits), 623 bytes captured (4984 bits) on interface 0 (ec2NFP_007AE807-180F-4A16-A802-68349A4E7DF2), id 0
> Ethernet II, Src: Shenzhen_53:8e:16 (1c:bfc:53:8e:16), Dst: MS-NL-PhysServer-01_a0:aa:31al (02:01:a0:ad:63:al)
> Internet Protocol Version 4, Src: 192.168.1.149 (192.168.1.149), Dst: protegermpc.net (192.0.78.25)
> Transmission Control Protocol, Src Port: 48396 (48396), Dst Port: https (443), Seq: 256817552, Win: 65535, Len: 4432, Len: 569

Transport Layer Security
▼ TLSv1.2 Record Layer: Application Data Protocol: http-over-tls
Content Type: Application Data (23)
Version: TLS 1.2 (0x0303)
Length: 564
Encrypted Application Data: 041b6372201b3f81b774d7ef4ee542a8ceea7302cc50b70d2...

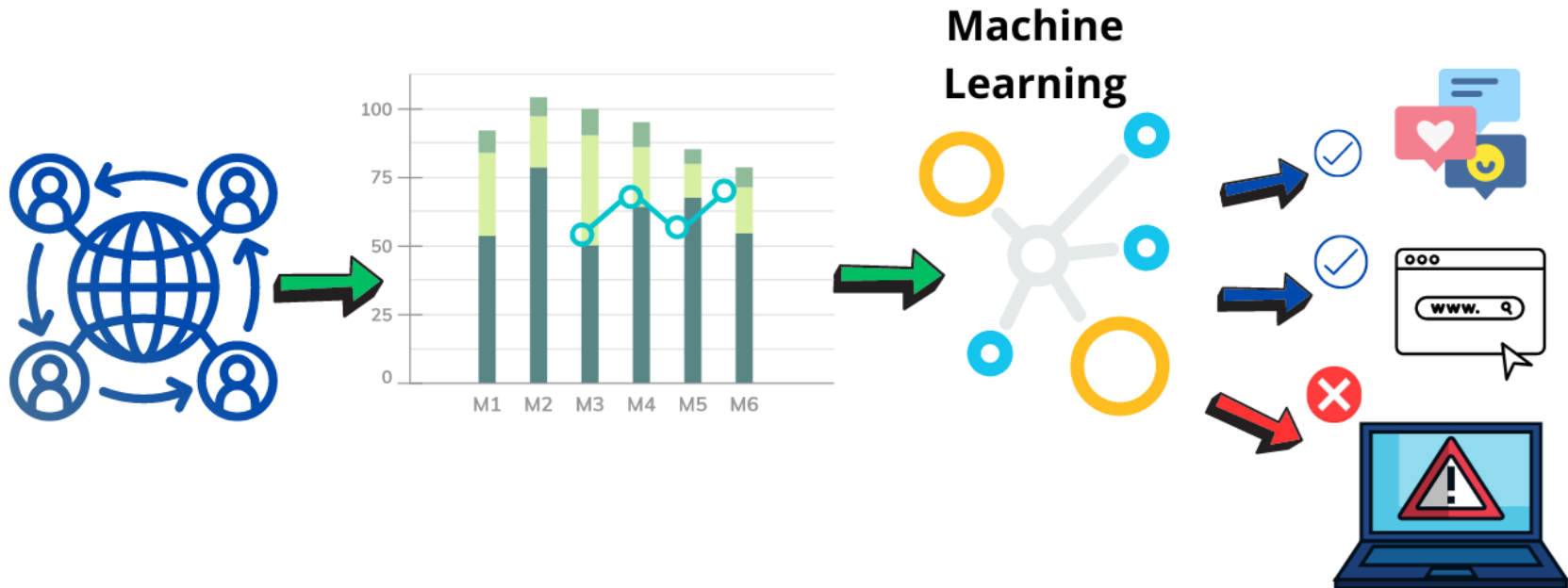
```
0030 f9 de d1 23 00 00 17 03 03 02 34 04 1b 63 72 20 ...E... .d.cr
0040 1d 3f 81 b7 f4 07 ef Ae e5 42 a8 ce ea 73 00 c0 ...?....M.B...s...
0050 5a 07 02 c9 47 72 f6 68 c3 55 f6 37 6f 70 08 08 ...j.... .ABVQu...
0060 01 aa e8 78 bd 46 56 b8 95 3f 8c 88 c4 f0 83 20 ...a..FV. ?.....
0070 f1 04 50 c9 07 05 21 78 c2 06 5b 27 90 42 36 f0 ...P...VIZ...[-]B...
0080 be a3 93 52 43 59 05 e5 0c 19 a5 5e 80 50 49 36 ...e...V... ..1...
0090 62 36 42 40 a6 e1 47 9a 08 f9 74 9b 52 27 ad 61 ...0000.G..h.t.R...
00a0 46 2c 7c 72 59 30 32 32 37 08 cc 05 28 59 09 f3 ...e...F...P...U...
00b0 2c c9 5b 08 40 72 28 cc ae aa 06 04 2b 95 78 32 ...?..0... ..F...j...
00c0 2f be aa 10 3c 0d 03 a6 35 80 93 2a c4 f0 3c 69 ...?.... .?....x...
00d0 1f 95 09 3d 13 68 19 e9 29 01 1e f0 81 5a 15 41 ...e...h... ..x...0...
00e0 33 8a c8 23 87 25 1f 04 4d 2a e3 9c c0 60 c0 ef ...3...S...M...m...
00f0 33 05 c7 06 f5 80 9f 2a 0f 04 08 02 08 9f ...S...e... ..e...
0100 a1 28 58 62 61 f6 bc ce 10 30 f8 9f 04 74 f9 24 ...Xob... ..0... ..
0110 04 42 86 98 08 4b c7 e8 19 3f a2 71 e5 7c 44 53 ...B...K... ..g... [0...
0120 11 8c 09 c8 71 c8 me cc ca 22 89 27 83 6f 05 64 ...e... ..e... ..e...
0130 15 69 08 f4 cb be dd 99 ef 8b 77 cf 42 96 51 93 ...i... .. ..B...Q...
0140 85 24 08 f9 5d 0f 9f 5f e7 c9 e8 75 c0 90 c3 96 ...S... ..M... ..u... ..
0150 06 52 89 44 87 c4 70 44 0f af 03 cb 0d 6a 98 22 ...e... ..e... ..d...
```

2. Inspección profunda de paquetes, es decir, la carga útil de los paquetes.

Marco Conceptual

Métodos de clasificación de tráfico

3. Aprendizaje automático usando datos estadísticos del tráfico de red.



Revisión Sistemática de la Literatura

RQ1. ¿Cuáles son los modelos de Machine Learning utilizados en la clasificación de ataques en SDN?

Técnica	EP1	EP2	EP3	EP4	EP5	EP6	EP7	EP8	EP9	EP10	EP11	EP12	EP13	EP14
Decision Tree														
Random Forest														
Support Vector Machine														
KNN														
Naive Bayes														
XG Boost														

Revisión Sistemática de la Literatura

RQ2. ¿Cuáles son las características utilizadas por las soluciones actuales en la clasificación de ataques en SDN?

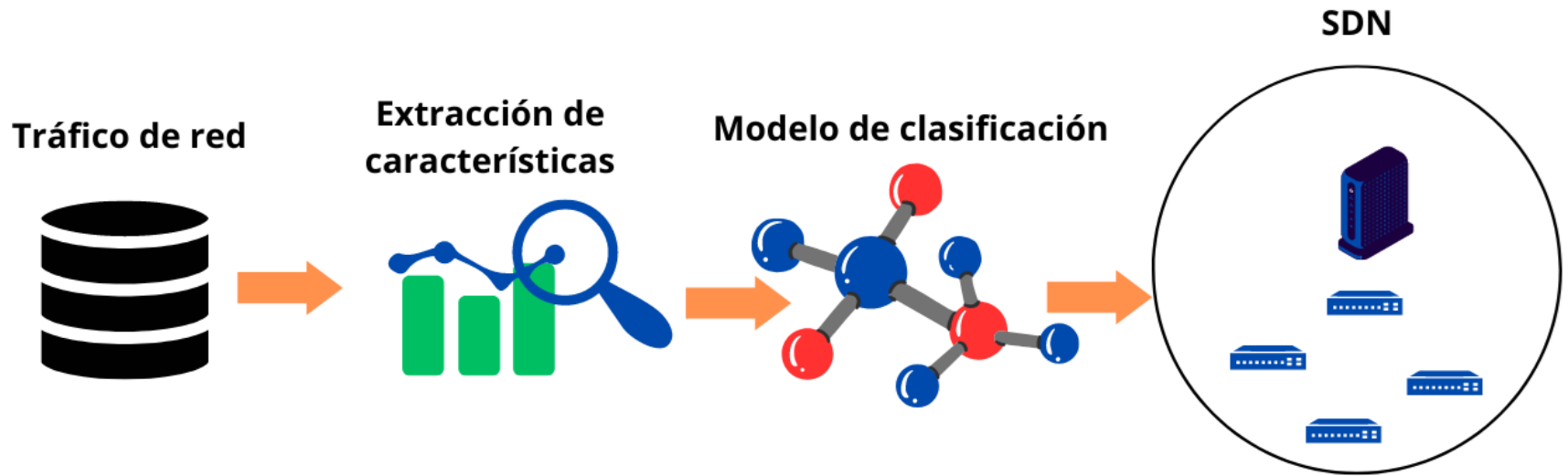
	EP1	EP2	EP3	EP4	EP5	EP6	EP7	EP8	EP9	EP10	EP11	EP12	EP13	EP14
Características		20	11	16		5		5	14		14	15		
Grupo de características			2											
Balaceo de Clases														

Revisión Sistemática de la Literatura

RQ3. ¿Cuáles son los conjuntos de datos disponibles para entrenar modelos de clasificación de ataques en SDN?

Dataset	Tipo de tráfico
NSL-KDD	DoS, Probe, R2L y U2R
CTU-13	Botnet
ISOT	DoS, Botnet, Ransomware
DDoS attacks SDN Dataset	DDoS
UNB-ISCX	DoS, DDoS, Ataques de Fuerza Bruta.
CSE-CIC-IDS2018	DoS, DDoS, Botnet, Heartbleed, Fuerza bruta y ataques web.

Propuesta de solución



Metodología

1. Investigación Científica del Diseño (Design Science Research, DSR)
2. Descubrimiento de conocimiento en bases de datos (Knowledge Discovery in Databases, KDD).
3. Análisis exploratorio de datos (Exploratory Data Analysis, EDA)

Metodología

1. Investigación Científica del Diseño

1. Identificación del problema

Ausencia de aplicaciones de seguridad en redes SDN debe detectar e identificar a tiempo los flujos malignos de la red.

2. Establecimiento de objetivos

Definir un modelo de clasificación de ataques usando técnicas de aprendizaje automático en Redes Definidas por Software

3. Diseño y desarrollo de la propuesta

- Desarrollo del modelo de clasificación
- Desarrollo de la arquitectura de implementación

4. Implementación

Despliegue del modelo de clasificación en un entorno SDN emulado.

5. Evaluación

Examinar el modelo de clasificación en un entorno de pruebas.

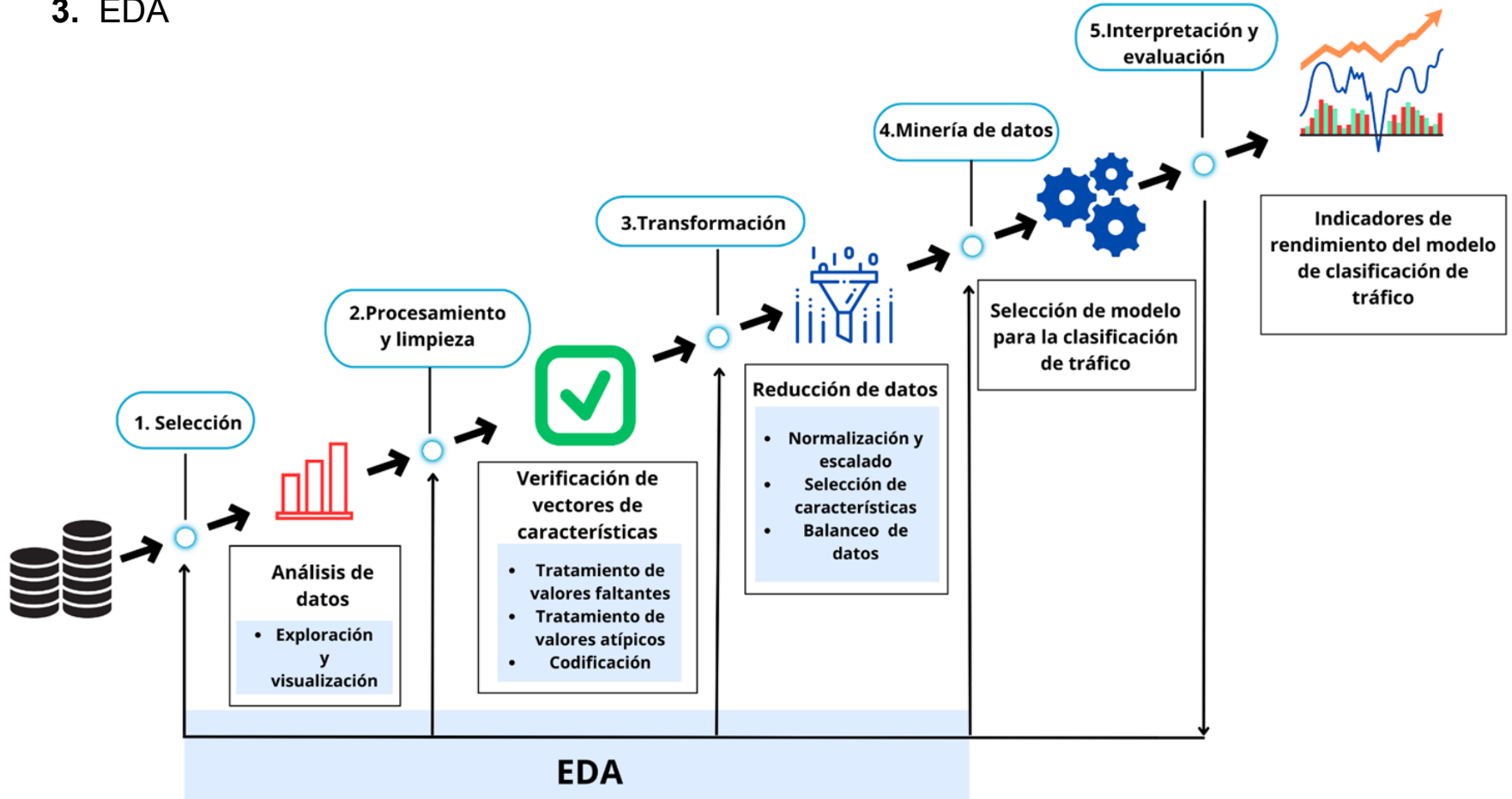
6. Resultados

Ponderaciones alcanzadas por el modelo de clasificación de tráfico.

Metodología

2. KDD

3. EDA



Desarrollo: origen de los datos

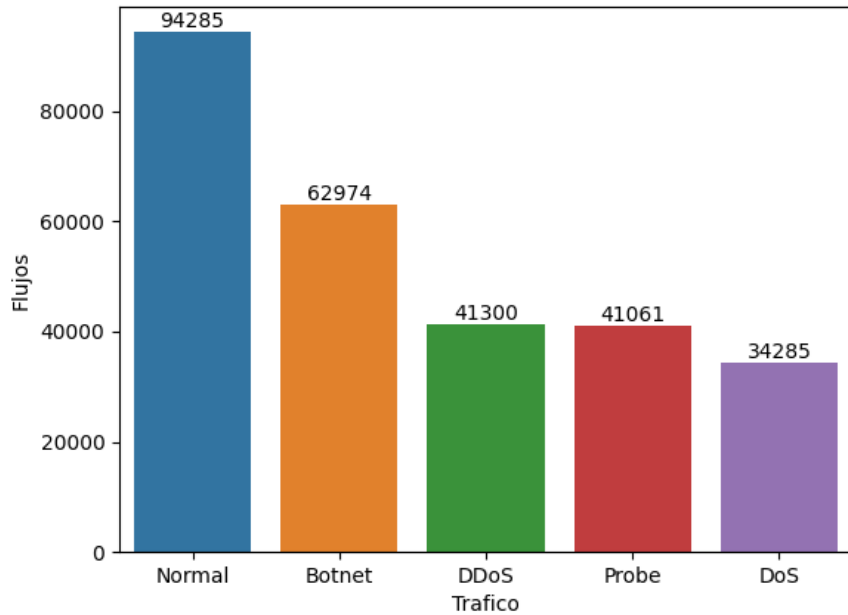
Extracción de características.

InSDN			
Tráfico	Cantidad	CICFlowMeter	Argus
Normal	68424	53784	111719
DoS	52471	33842	35030
DDoS	48413	398643	3352394
Probe	36372	41980	49452
Botnet	164	92	193

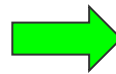
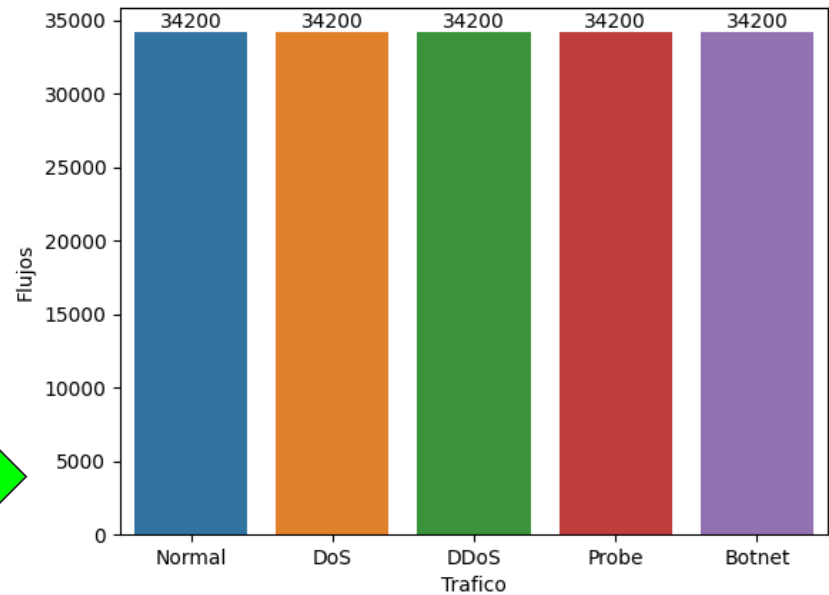
CTU-13			
Tráfico	Cantidad	CICFlowMeter	Argus
Botnet	2753290	132168	192168

Desarrollo: limpieza de datos

Cantidad de datos sin valores faltantes.



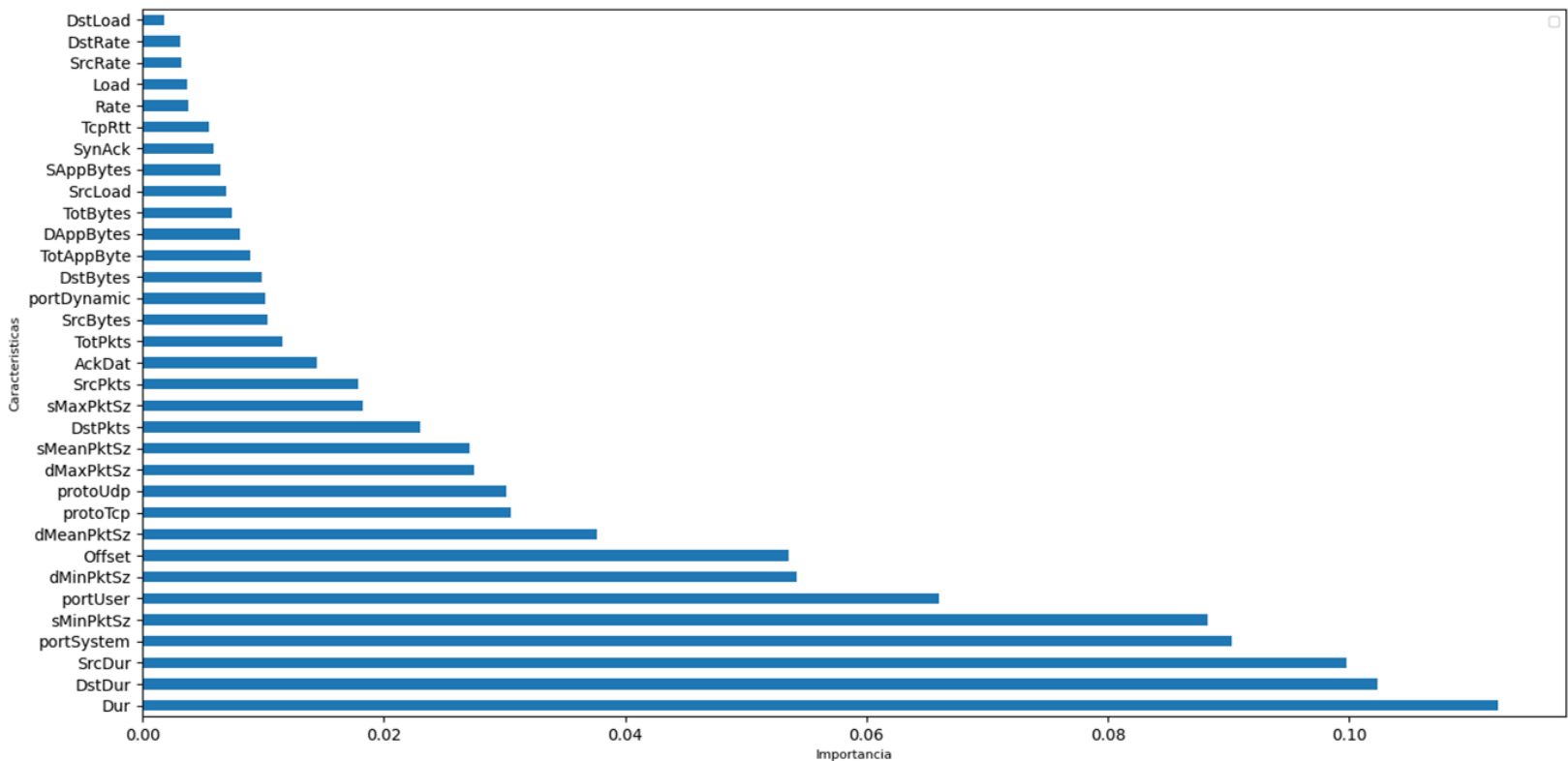
Cantidad de datos equilibrados



Desarrollo: selección de características

1. Matriz personalizada para seleccionar características.
2. Select K-Best
3. Matriz de Correlación
4. Análisis de Componentes Principales

Ponderación de características:



Desarrollo: selección de características

Definición de conjuntos de características.

GRUPO	NÚMERO	CARACTERÍSTICAS
FG1	9	Dur, Proto, Dport, TotPkts, SrcPkts, DstPkts, TotBytes, SrcBytes, DstBytes
FG2	12	Dur, Proto, Dport, TotPkts, SrcPkts, DstPkts, TotBytes, SrcBytes, DstBytes, Rate, SrcRate, DstRate
FG3	20	Dur, SrcDur, DstDur, Proto, Dport, TotPkts, SrcPkts, DstPkts, TotBytes, SrcBytes, DstBytes, Rate, SrcRate, DstRate, sMeanPktSz, dMeanPktSz, sMaxPktSz, dMaxPktSz, sMinPktSz, dMinPktSz
FG4	14	Dur, SrcDur, DstDur, Proto, Dport, TotPkts, SrcPkts, DstPkts, TotBytes, SrcBytes, DstBytes, Rate, SrcRate, DstRate

Desarrollo: selección de modelos

Análisis de selección de modelos:

MODELO ML	VENTAJA	DESVENTAJA	EJECUCIÓN
NAIVE BAYES	IMPLEMENTACIÓN FÁCIL	POCOS PARÁMETROS	MEDIA
RANDOM FOREST	ALTO RENDIMIENTO	SOBREAJUSTE	MEDIA
REGRESIÓN LOGÍSTICA	SALIDA VARIADA	SUPONE	RÁPIDO
SVM	EFICIENTE	RESULTADOS BAJOS	LENTO
DECISION TREE	ALTO RENDIMIENTO	SOBREAJUSTE	RÁPIDO
KNN	DEDUCCIÓN RÁPIDA	ENCONTRAR N VECINOS	MEDIA



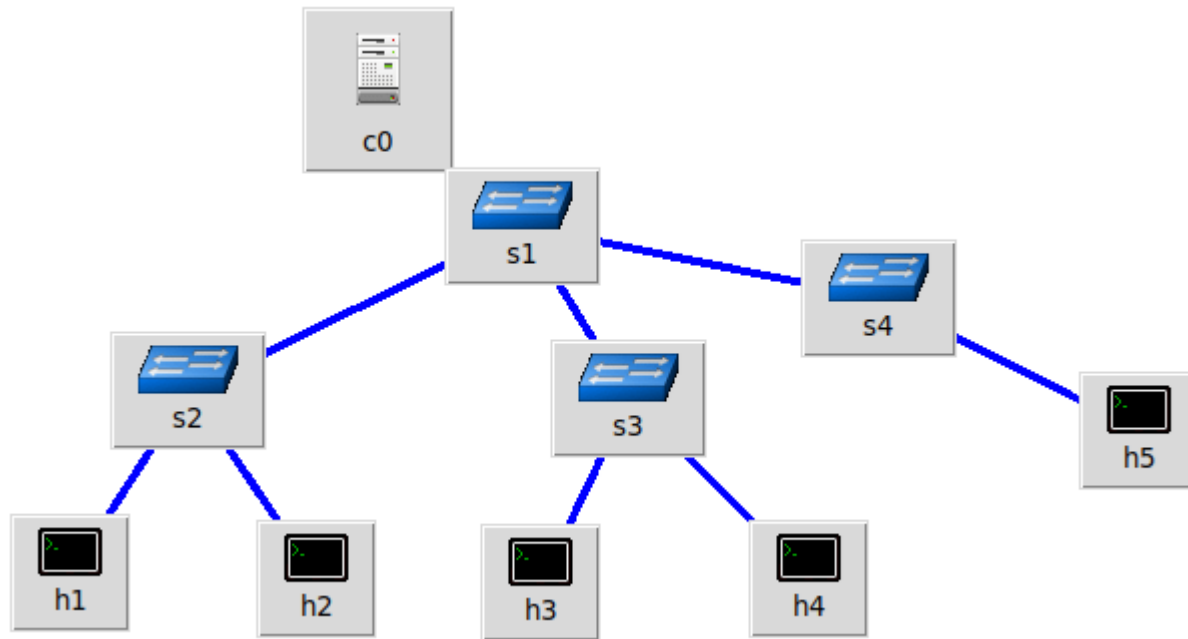
Desarrollo: entrenamiento del modelo

Resultados de hiperparámetros por modelo de clasificación:

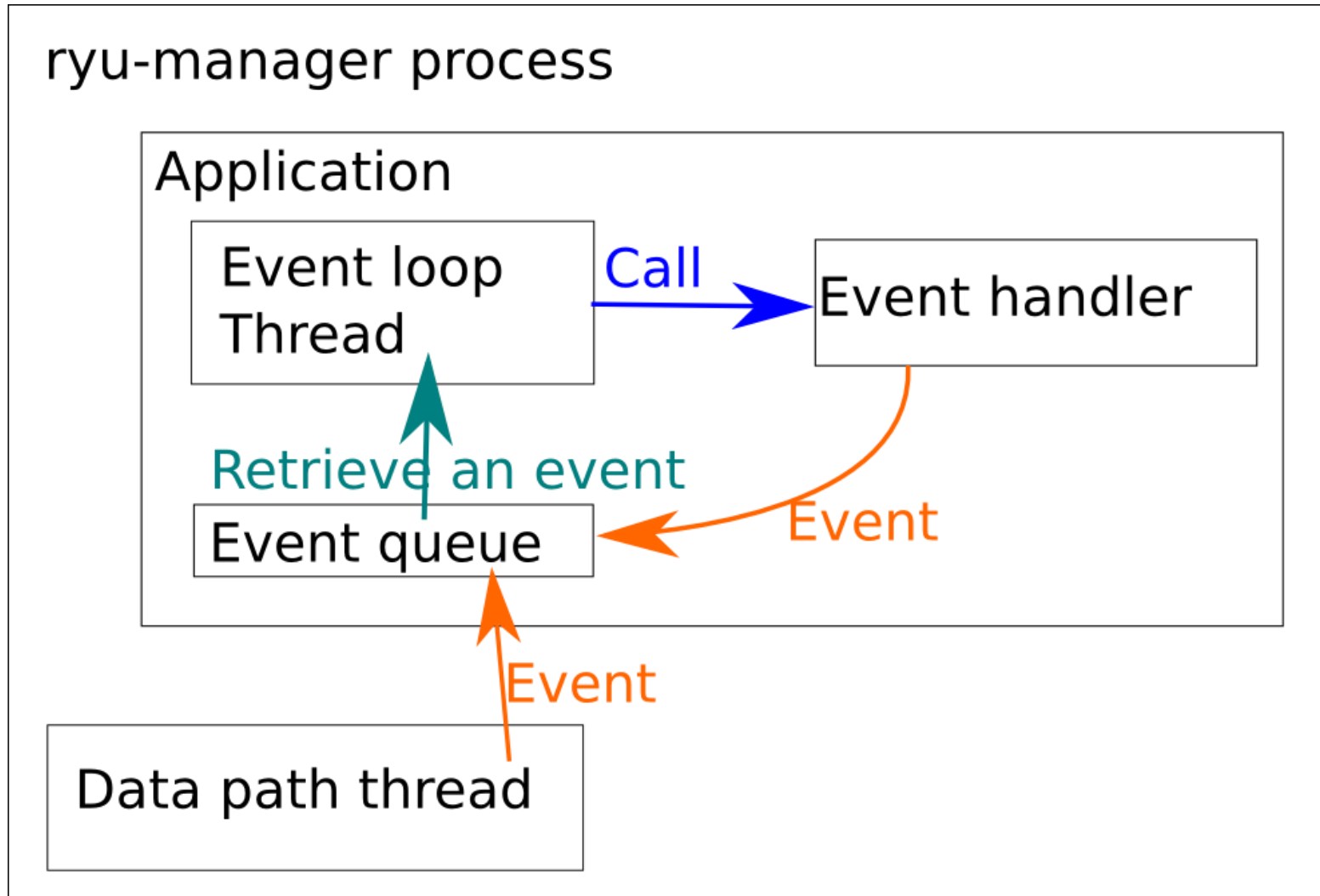
MODELO	HYPERPARÁMETRO	VALOR
DECISION TREE	CRITERION MAX_DEPTH MIN_SAMPLES_SPLIT MIN_SAMPLES_LEAF CCP_ALPHA SPLITTER	ENTROPY 12 2 1 0.0001 BEST
RANDOM FOREST	N_ESTIMATORS CRITERION MAX_DEPTH MIN_SAMPLES_SPLIT MIN_SAMPLES_LEAF CCP_ALPHA	10 ENTROPY 12 5 2 0.0001
SVM	C KERNEL GAMMA DECISION_FUCTION_S HAPE	1000 RBF SCALE OVO

Implementación

- Topología de red SDN



Controlador Ryu



Recuperado de Ryubook 1.0 documentation (2023).

Funcionamiento del modelo de clasificación

Algoritmo 1 Clasificación de flujos

1: **procedure** CONEXION CONTROLADOR Y APLICACION DE MODELO DE CLASIFICACION

Require: *IP del servidor de aplicacion*

2: **procedure** GESTIÓN DE ESTADÍSTICAS DE FLUJO

Require: *Controlador envia solicitud de estadísticas de flujo al Switch*

3: *Controlador* ← *Mensaje*

4: **while** *Mensaje = TCP or UDP do*

5: *ListaMensajes* ← *Mensaje*

6: **if** *len(ListaMensajes)%2 == 0 then*

7: **for** *Caracteritica in ListaMensajes do*

8: **if** *Duracion ≤ 20s then*

9: *Flujo1* ← *Caracteristica*

10: *Flujo2* ← *Caracteristica + 1*

11: *FlujoBidireccional* ← *Flujo1 + Flujo2*

12: *POST* ← *FlujoBidireccional*

13: *Modelo* ← *POST*

14: *Respuesta* ← *Modelo*

15: *Controlador* ← *Respuesta*

16: **end if**

17: **end for**

18: **end if**

19: **end while**

20: **end procedure**

21: **end procedure**

Resultados

Resultados de entrenamiento y validación del modelo.

Modelo	Accuracy de Entrenamiento	Accuracy de Validación
9 Características		
DT	99.34%	99.28%
RF	99.31%	99.31%
SVM	96.83%	96.83%
12 Características		
DT	99.28%	99.25%
RF	99.36%	99.30%
SVM	96.91%	97.09%

Modelo	Accuracy de Entrenamiento	Accuracy de Validación
14 Características		
DT	99.80%	99.76%
RF	99.76%	99.75%
SVM	99.49%	99.50%
20 Características		
DT	99.25%	99.25%
RF	99.32%	99.25%
SVM	97.06%	97.06%

Resultados

Resultados de la implementación del modelo de clasificación con captura de tráfico en directo.

Características	DT	RF	SVM
9	20.02%	21.45%	27.33%
12	24.14%	23.97%	43.28%

Conclusiones

- ❖ Se desarrollaron tres modelos de aprendizaje automático para la clasificación de tráfico normal, DoS, DDoS, probe y botnet. Las técnicas utilizadas fueron DT, RF y SVM, entrenadas con 136800 muestras. El conjunto de datos utilizado para entrenar los modelos resultó de la combinación entre InSDN y CTU-13, para el tratamiento de los datos se aplicó las metodologías KDD y EDA.
- ❖ Según el SLR existen diversas ideas para desarrollar modelos que puedan clasificar ataques de tráfico en SDN; muchos de estos estudios se centran en la detección de tráfico, es decir, en su mayoría manejan dos tipos de tráfico: normal y de ataque. Por lo general, el tráfico de ataque se centra únicamente en DDoS. Además, los conjuntos de datos en su mayoría no son de origen SDN.

Conclusiones

- ❖ Para la implementación del modelo de clasificación de ataques, se utilizó Mininet, Ryu y Flask. En Mininet se desarrolló la topología, la cual representa el plano de datos. En cambio, Ryu es el controlador que permite gestionar el tráfico de la red. Por último, Flask permite desplegar el modelo de clasificación de ataques y escenifica el plano de aplicación.
- ❖ Los resultados encontrados durante el entrenamiento de los modelos DT, RF y SVM fueron del 99.76%, 99.31% y 99.50% de precisión, respectivamente. Estos hallazgos son obtenidos a partir de la validación del modelo y no del resultado del entrenamiento, como se realiza en algunos trabajos relacionados. Además, se implementó el modelo en un entorno de emulación, y se obtuvo 43.28%, 24.14% y 23.97% para los modelos SVM, DT y RF, respectivamente.

Recomendaciones

- ❖ Analizar los datos de origen y utilizar metodologías interactivas para el tratamiento de los datos.
- ❖ Se recomienda conocer qué tipos de datos aceptan los algoritmos y si estos son sensibles al ruido de los datos, sobreajuste o desajuste.
- ❖ Para el despliegue de un modelo de clasificación de tráfico, se recomienda conocer las características que ofrece el controlador, así como también, los módulos, clases, eventos y APIs. Dado que para el modelo con cualquier tipo de aprendizaje, la aplicación en el controlador es un requisito importante, porque desde allí se extraen las características y el funcionamiento de toda la red.

Trabajos Futuros

- ❖ Para mejorar los resultados del modelo de clasificación y realizar su implementación en una red SDN, se podría aumentar el conjunto de datos. Además, se debería analizar la existencia de nuevas características en distintas versiones de controladores open source.
- ❖ Una de las posibles mejoras para trabajos futuros es la aplicación de técnicas de aprendizaje profundo para entrenar el modelo de clasificación de ataques, lo que permitiría detectar patrones en los datos de forma más eficiente y precisa. El uso de estas técnicas podría mejorar significativamente el nivel de predicción del modelo.

Muchas gracias