Efecto de la selección de atributos en el desempeño de un IDS basado en machine learning para detección de intrusos en ataques DDoS

Effect of attribute selection on the performance of a machine learning-based IDS for intrusion detection in DDoS attacks

DOI: 10.46932/sfjdv4n2-023

Received in: April 04th, 2023
Accepted in: May 05th, 2023

José Albeiro Montes-Gil
MSc. in Information Systems Administration
Institución: Universidad Nacional de Colombia
Dirección: LIGRED Laboratory, Campus La Nubia. Universidad Nacional de Colombia, Manizales Caldas Colombia
Correo electrónico: joamontesgi@unal.edu.co

Gustavo Isaza-Cadavid
PhD Ingeniería de Software
Institución: Universidad Pontificia de Salamanca
Dirección: Calle 65, No. 26-10, Universidad de Caldas - Facultad de Ingenierías, Manizales, Colombia
Correo electrónico: gaisaza@ucaldas.edu.co

Néstor Darío Duque-Méndez
PhD Ingeniería
Institución: Universidad Nacional de Colombia
Dirección: Universidad Nacional de Colombia - Depto de Informtica y Computación, Manizales Colombia
Correo electrónico: ndduqueme@unal.edu.co

RESUMEN
En sistemas informáticos cada vez más expuestos a través de redes globales de comunicación, la ciberseguridad enfrenta grandes retos. Dentro de los riesgos a que están expuestos estos sistemas están los ataques de denegación de servicios DoS, que atentan con la disponibilidad de los recursos. Dentro de los mecanismos para enfrentar esta situación están los sistemas de detección de intrusos IDS que mediante análisis de las tramas entrantes intentan determinar la presencia de un ataque. Los enfoques basados en técnicas de inteligencia artificial y algoritmos de machine learning muestran una contribución importante en la implementación de IDS en la actualizada. Pero como en todos los algoritmos de machine learning la alta dimensionalidad de los datos, como en el caso de las tramas en la red, pueden afectar el desempeño en el entrenamiento y más aún en la fase de producción. Las estrategias de reducción de características son una alternativa aplicada en muchos campos para poder seleccionar características que mantengan el buen desempeño de los algoritmos, pero mejorando el rendimiento. Este articulo presenta el efecto de la selección de atributos en el desempeño de un IDS basado en machine learning para detección de intrusos en ataques DDoS, mediante estudio empírico. El dataset utilizado es CICIDS-2017.

Palabras clave: ciberseguridad, ataques DoS, sistemas de detección de intrusos, selección de características.

ABSTRACT
In computer systems that are increasingly exposed through global communication networks, cybersecurity faces great challenges. Among the risks to which these systems are exposed are DoS denial of service attacks, which threaten the availability of resources. Among the mechanisms to deal with this situation are the IDS intrusion detection systems that try to determine the presence of an attack by analyzing the incoming frames. The approaches based on artificial intelligence techniques and machine learning algorithms show an important contribution in the implementation of IDS in the updated one. But as in all machine learning algorithms, the high dimensionality of the data, as in the case of the frames in the network, can affect the performance in training and even more so in the production phase. Feature reduction strategies are an alternative applied in many fields to be able to select features that maintain the good performance of algorithms but improve performance. This article presents the effect of attribute selection on the performance of an IDS based on machine learning for intrusion detection in DDoS attacks, through an empirical study. The dataset used is CICIDS-2017.

Keywords: cybersecurity, DoS attacks, intrusion detection systems, feature selection.

1 INTRODUCCIÓN

En un mundo cada vez más interconectado a través de redes de computadores, la seguridad informática es fundamental. La Ciberseguridad se asocia con las medidas que se implementan buscando la protección de los recursos tecnológicos ante ataques digitales, evitando la divulgación, destrucción o modificación no deseada de la información o componentes técnicos (Humayun et al., 2020). En general se espera garantizar la privacidad de los datos y la información, mantener el correcto funcionamiento de un servicio y dar confianza sobre lo entregado por los sistemas. Podemos decir que se busca garantizar la disponibilidad, la confidencialidad y la confiabilidad de los sistemas (Quiroz & Valencia, 2017), (Humayun et al., 2020).

Los ataques de Denegación de Servicios (DoS) se orientan a afectar la disponibilidad de un recurso o servicio, impidiendo el acceso parcial o total a los usuarios. Un ataque DoS se consigue con el envío de una gran cantidad de peticiones hasta que el equipo víctima no pueda procesar de manera exitosa todas las solicitudes recibidas, esto puede provocar colapsos en los recursos del sistema (Hadeel S. Obaid, 2020).

Los ataques de denegación de servicio distribuido (DDoS) son una de las amenazas más comunes en la seguridad de redes.

Para combatir estos ataques, se han desarrollado diversas técnicas, entre ellas, la utilización de sistemas de detección de intrusos (IDS), que mediante el examen permanente de las tramas que ingresan pueden determinar si en algún momento está comprometida la seguridad. El uso de IDS para la mitigación en ataques DDoS se puede observar en (Sallam et al., 2020), (Almseidin & Kovacs, 2019), (Manso et al., 2019) y (Chaudhary & Shrimal, 2019).

Uno de los enfoques que han demostrado buenos desempeños para detectar y prevenir estos ataques está relacionado con el uso de algoritmos de inteligencia artificial, específicamente de machine learning (ML) de aprendizaje supervisado para predecir posibles ataques. El desempeño de los algoritmos de machine learning depende de muchos factores, entre ellos uno de interés para este artículo: Las características involucradas en el proceso de entrenamiento para obtener un modelo generalizable, que teóricamente son un factor crítico que puede afectar significativamente el rendimiento.

En este artículo se presenta el efecto de la selección de atributos en el desempeño de un IDS basado en machine learning para detección de intrusos en ataques DDoS. Se realiza un estudio empírico que evalúa el desempeño del modelo con diferentes clasificadores para determinar el efecto de la reducción de atributos en las métricas de predicción y los tiempos de ejecución. El dataset utilizado es CICIDS-2017 fue creado por la Universidad de Nueva Brunswick en el año 2017 (Panigrahi & Borah, 2018).

Los resultados obtenidos muestran la importancia de la selección adecuada de atributos en el desempeño del IDS basado en machine learning, lo que se considera el aporte de este trabajo y pueden ser de utilidad para mejorar la eficacia de los sistemas de detección de intrusiones en la lucha contra los ataques DDoS.

El resto del artículo está organizado de la siguiente manera: En la sección 2 se presentan algunos trabajos de interés para este artículo; en la siguiente sección se presenta el marco experimental, seguido de los resultados obtenidos y su discusión respectiva, para finalizar en la sección 5 con las conclusiones y trabajo futuro.

2 TRABAJOS RELACIONADOS

Son varias las investigaciones y enfoques que se encuentran en la literatura sobre el uso de algoritmos de inteligencia artificial y ML para la implementación de sistemas de ciberseguridad y en particular para sistemas de detección de intrusos. A continuación, se enumeran algunos de ellos, que sirvieron para definir el marco de trabajo de este artículo.

En (Lee et al., 2020) los autores presentan un sistema de detección y prevención de intrusos (IDPS) orientado a ataques de fuerza bruta y DDos para redes definidas por software. Se aplican y comparan redes neuronales convolucionales, perceptrones multicapas (MLP), memoria a largo plazo (LSTM). El IDPS basado en MLP llega a una precisión del 99% en la prevención de ataques de fuerza bruta y casi el 100% en DDoS.

Los autores en (Dong et al., 2022) proponen la detección de tráfico anómalo usando el dataset NSL-KDD mediante un autocodificador variacional. El modelo está compuesto de 2 etapas: preprocesamiento de los datos, y la predicción por medio del modelo. Se comparan la precisión, exhaustividad, puntaje F1 y exactitud entre los clasificadores Bosque Aleatorio (RF), Máquina de Soporte

Vectorial (SVM), Regresión Logística (LR) y Perceptrón Multicapa (MLP). A pesar de los buenos resultados, se recomienda aumentar el número de instancias para el conjunto de entrenamiento, si el objetivo es aumentar la precisión del modelo (87.27%).

En (Muraleedharan & Janet, 2021) se define un modelo para clasificar ataques DoS tipo Slow con técnicas de aprendizaje profundo, usando el dataset CICIDS2017.

En (Ortiz y otros, 2020) se presenta trabajo donde aplican Boruta e Importancia de la Permutación para la selección de características en el dataset CICIDS-2017, aplicando diferentes técnicas de aprendizaje supervisado para obtener la precisión de cada uno de los clasificadores, entre los que se resaltan Random Forest y Árboles de Decisión. Los autores mencionan la importancia de continuar realizando análisis con otro tipo de clasificadores y selectores de características.

En (Hua, 2020) se construyó un esquema para un IDS dividido en 2 etapas: preprocesamiento, con selección de características y creación del modelo. En la segunda etapa se realizaron comparaciones entre las salidas de Máquinas de Vectores de Soporte, Random Forest, Redes Neuronales Convolucionales, Perceptrón Multicapa, entre otros.

En (Iram y otros, 2020) los autores usaron el conjunto de datos NSL-KDD con las características aleatorias para reducir la cantidad de atributos, los tiempos de entrenamiento y la complejidad del modelo. Se implementaron 8 técnicas de ML, con buenos resultados en predicción de ataques DoS, mientras que en ataques U2R su rendimiento fue inferior. Como trabajos futuros, se menciona la importancia de implementar diferentes métodos para la Selección de Características para disminuir la complejidad computacional de las propuestas de IDS.

Si bien la reducción de características puede generar una reducción en la complejidad de un modelo, en (Nazir y Khan, 2021) se observa un rendimiento más alto en términos de precisión cuando el número de atributos aumenta. En (Mahmood, Abdi y Hussin, 2021) se analizó el rendimiento de algunos algoritmos que aplicaban selección de características, de allí se concluye que la precisión de los modelos puede ser incrementada en algunos casos a medida que aumenta el número de características.

En (Montes et al., 2023) se presentan los resultados de aplicar diferentes algoritmos para obtener subconjuntos de características que mantienen un buen desempeño en las tareas de clasificación. Los resultados muestran que en los diferentes clasificadores todas las métricas disminuyen cuando se reduce en gran medida el número de características, pero que con la operación unión de los subconjuntos de características obtenidos a partir de la importancia de las características, el número de atributos obtenidos se reduce significativamente y se mantiene el buen desempeño del clasificador.

Esta breve revisión permite observar que la selección de características en conjuntos de datos relacionados con seguridad informática es un campo de interés y puede aportar mejoras al rendimiento de los modelos de clasificación, cuando estos se basan en inteligencia artificial y ML, pero excepto en

(Montes et al., 2023) no se reporta un subconjunto de características optimo en los diferentes clasificadores.

3 MARCO EXPERIMENTAL

En esta sección se exponen los componentes involucrados en el estudio empírico.

3.1 DATASET UTILIZADO

El conjunto de datos CICIDS2017 es un dataset elaborado por investigadores del Instituto Canadiense para la Ciberseguridad de Universidad de Nueva Brunswick en el año 2017 y fue diseñado para ayudar a la creación de modelos para la detección de ataques informáticos (Panigrahi & Borah, 2018). Este dataset contiene un total de 78 columnas y captura de 2’827.876 registros.

El dataset registra diferentes tipos de ataques, no obstante, este artículo se centra sólo en los ataques DoS/DDoS. Finalmente queda reducido a un total de 78 atributos (incluyendo el atributo clase) y 1’447.279 instancias.

Los atributos en el dataset se presentan en la tabla 1.

Tabla 1. Atributos CIDS2017 - DatasetTodos

Nombre	Columna CICIDS2017	Nombre	Columna CICIDS2017	Nombre	Columna CICIDS2017
1	dst_port	27	bwd_iat_mean	53	pkt_size_avg
2	flow_duration	28	bwd_iat_std	54	fwd_seg_size_avg
3	tot_fwd_pkts	29	bwd_iat_max	55	bwd_seg_size_avg
4	tot_bwd_pkts	30	bwd_iat_min	56	fwd_byts_b_avg
5	totlen_fwd_pkts	31	fwd_psh_flags	57	fwd_pkts_b_avg
6	totlen_bwd_pkts	32	bwd_psh_flags	58	fwd_blk_rate_avg
7	fwd_pkt_len_max	33	fwd_urg_flags	59	bwd_byts_b_avg
8	fwd_pkt_len_min	34	bwd_urg_flags	60	bwd_pkts_b_avg
9	fwd_pkt_len_mean	35	fwd_header_len	61	bwd_blk_rate_avg
10	fwd_pkt_len_std	36	bwd_header_len	62	subflow_fwd_pkts
11	bwd_pkt_len_max	37	fwd_pkts_s	63	subflow_fwd_byts
12	bwd_pkt_len_min	38	bwd_pkts_s	64	subflow_bwd_pkts
13	bwd_pkt_len_mean	39	pkt_len_min	65	subflow_bwd_byts
14	bwd_pkt_len_std	40	pkt_len_max	66	init_fwd_win_byts
15	flow_byts_s	41	pkt_len_mean	67	init_bwd_win_byts
16	flow_pkts_s	42	pkt_len_std	68	fwd_act_data_pkts
17	flow_iat_mean	43	pkt_len_var	69	fwd_seg_size_min
18	flow_iat_std	44	fin_flag_cnt	70	active_mean
19	flow_iat_max	45	syn_flag_cnt	71	active_std
20	flow_iat_min	46	rst_flag_cnt	72	active_max
21	fwd_iat_tot	47	psh_flag_cnt	73	active_min
22	fwd_iat_mean	48	ack_flag_cnt	74	idle_mean
23	fwd_iat_std	49	urg_flag_cnt	75	idle_std
24	fwd_iat_max	50	cwe_flag_count	76	idle_max
25	fwd_iat_min	51	ece_flag_cnt	77	idle_min
26	bwd_iat_tot	52	down_up_ratio	78	**Label**

3.2 SELECCIÓN DE CARACTERÍSTICAS

La selección de características es una estrategia implementada en conjuntos de datos grandes que busca generar una reducción en la dimensionalidad de un problema, de tal forma que se pueden obtener mejores o equivalentes resultados con mejores relaciones de costo computacional (Iram et al., 2020).

Para este estudio experimental se tomó como referencia el trabajo en (Montes et al., 2023), donde a través de diferentes estrategias sobre las características se logra establecer que un subconjunto de atributos, producto de la unión de los resultados que establecen la importancia de las características usando diferentes clasificadores (Random Forest, XGB y árboles de decisión), es una alternativa válida en contraposición al uso de todos los atributos.

De el total de características mostradas en la tabla 1 el subconjunto propuesto es de 37 atributos, como se aprecia en la tabla 2.

Tabla 2. Subconjunto de atributos CIDS2017 - - DatasetUnion

Subconjunto	**Características**
subconjunto_unión	0, 1, 3, 4, 5, 6, 7, 9, 10, 11, 13, 14, 15, 16, 17, 18, 20, 21, 22, 23, 24, 25, 27, 34, 35, 36, 38, 42, 62, 65, 67, 69, 71, 72, 73, 75, 76

Para los experimentos se aplicarán diferentes algoritmos de machine learning tanto sobre el dataset completo (DatasetTodos) como sobre el subconjunto (DatasetUnion). Para evitar overfitting se dividen las instancias en de entrenamiento (80%) y de prueba (20%), quedando 1’157.823 instancias para entrenamiento y para test 289.456.

3.3 ALGORITMOS DE MACHINE LEARNING

Machine Learning o aprendizaje automático es la práctica de programar computadores para que aprendan de los datos. En el aprendizaje automático, los datos se denominan conjuntos de entrenamiento o ejemplos (Russell, 2018). El Aprendizaje Supervisado es una agrupación del Aprendizaje de Máquina (Machine Learning) el cual permite detectar un comportamiento normal o atípico en un conjunto de datos (Maldonado, 2018). Una de las características más importantes del Aprendizaje Supervisado es la posibilidad de generar predicciones a partir de cálculos matemáticos, donde se conoce cuál es la característica de un objeto y se conoce su clase (Correa Wachter & Henao Villas, 2021).

Retomando el trabajo en En (Virupakshar et al., 2020) se seleccionaron para los experimentos, que tienen como finalidad principal hacer la comparación de los resultados relativos según el número de características utilizados y evaluar la capacidad de los algoritmos en forma individual en cuanto a las métricas obtenidas.

A continuación, se exponen rápidamente los algoritmos a implementar en este trabajo (Bramer, 2013).

K Vecinos Cercanos (K Nearest Neighbor - KNN): Es un algoritmo de clasificación ampliamente usado en tareas de predicción. Tiene como ventaja que no requiere grandes volúmenes de datos para su entrenamiento, pero, su costo está en la etapa de validación.

Árboles de Decisión (Decision Tree - DT): Es un algoritmo de clasificación no paramétrica que genera predicciones a partir del uso de reglas basadas en la agrupación de criterios, bajo un único nodo inicial y una ramificación a partir de los resultados. CART (Árbol de clasificación y regresión) es una variación del algoritmo del árbol de decisión. Puede manejar tareas de clasificación y regresión.

Naïve Bayes: Es un algoritmo de aprendizaje supervisado, que se basa en el teorema de Bayes y se utiliza para resolver problemas de clasificación. Es simple y efectivo en la construcción de modelos de aprendizaje automático en forma rápida.

Bosque Aleatorio (Random Forest): es una técnica de aprendizaje supervisado que genera varios árboles de decisión para la fase de entrenamiento con divisiones de subnodos en forma aleatoriamente para reducir el sobreentrenamiento.

4 RESULTADOS Y DISCUSION

Manteniendo el marco experimental y luego de realizar varias corridas en diferentes momentos, para cada uno de los algoritmos y cada uno de los dataset se obtuvieron los resultados promedios mostrados en la tabla 3.

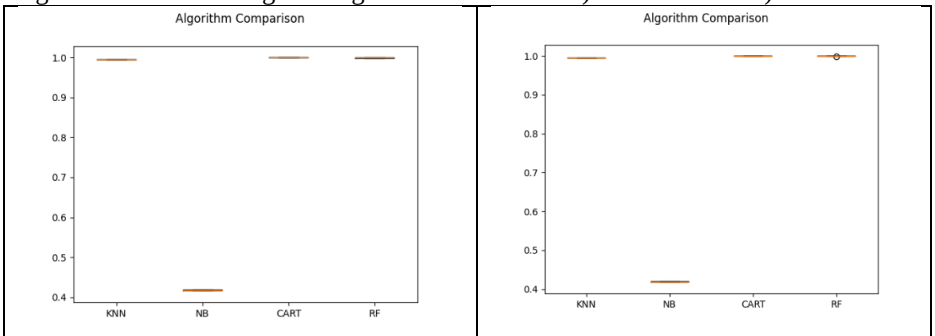
Tabla 3. Resultados de Score, desviación estándar y tiempo de ejecución

	KNN	Std	t (seg)	NB	Std	t (seg)	CART	Std	t (seg)	RF	Std	t (seg)
DatasetTodos	0,99542	0,000142	19370,44	0,417396	0,001041	30,535	0,999558	0,000041	4172,255	0,999526	0,000054	3555,32
DatasetUnion	0,99539	0,000145	10237,13	0,419144	0,000965	17,03	0,999552	0,00005	1720,16	0,999524	0,00007	475,13

Es notorio que en todos los casos la desviación estándar es muy pequeña.

En la figura 1, en el gráfico de bigotes se observa que el comportamiento de los algoritmos tanto para el datasetTodos como para el datasetUnion es muy parecido.

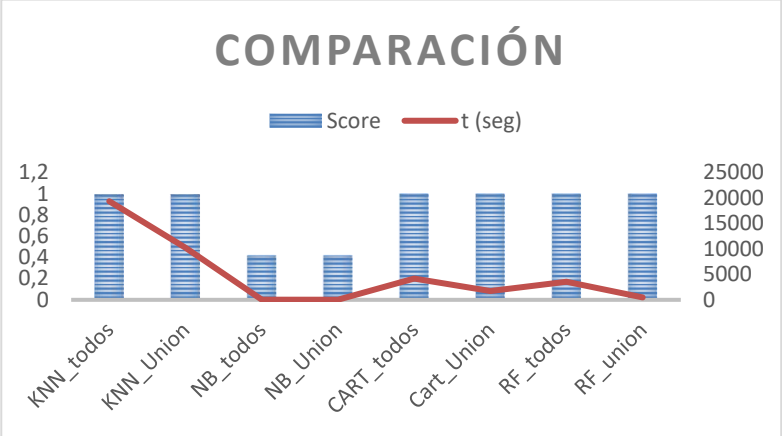
Figura 1. Gráfica de bigotes Algoritmos / Datasets. a) DatasetTodos b) datasetUnion



a) DatasetTodos | b) DatasetUnion

En la figura 2 se aprecia los resultados de score para cada algoritmo y el tiempo requerido para la ejecución completa. Representan el promedio de las corridas.

Figura 2. Resultados métricas y tempos de ejecución



Con el fin de tener otros elementos de juicio este mismo proceso se hizo utilizando 2 ambientes diferentes: Ejecución en Google Colab y un portátil personal y se pudo comprobar el comportamiento analizado se mantiene, desde luego con cambios en los valores absolutos, especialmente en los tiempos de corrida.

Con el fin de no dejar de lado otros algoritmos que son fuertemente referenciados en la literatura se aplicó el mismo procedimiento con redes neuronales simples y perceptrones multicapa (MLP), esta última con 2 capa ocultas y 3 neuronas en cada una. Los resultados promedios se aprecian en la tabla 4 y siguen el mismo comportamiento con respecto al número de atributos en el entrenamiento.

Tabla 4. Resultados de Score, desviación estándar y tiempo de ejecución para redes neuronales

	NN	Std	t (seg)	MLP	Std	t (seg)
DatasetTodos	0,85813	0,09051	486,649	0,76101	0,02875	1620,7
DatasetUnion	0,79278	0,05494	259,273	0,7436	0,01296	847,82

Como se aprecia en los diferentes escenarios de la experimentación el comportamiento es parecido, lo que permite afirmar, sin ser concluyente, que con los resultados con el dataset reducido mediante técnicas de feature selection y propuesto en [], que hemos denominado datasetUnion (37 características), el desempeño de la métrica score es muy cercano, en todos los casos, al valor respectivo obtenido con el número total de atributos (78).

5 CONCLUSIONES Y TRABAJO FUTURO

Es reconocida en la literatura la importancia de los IDS como un mecanismo de seguridad ante ataques de denegación de servicios. Dentro de los enfoques para la construcción de IDS se encuentran los que se basan en técnicas de inteligencia y machine learning, aplicando diferentes algoritmos.

En la ejecución de estos algoritmos el costo computacional se incrementa en la medida que los datasets crecen en número de instancias o número de características. La selección de características es un enfoque que trata de enfrentar esta situación, permitiendo tener el mínimo número de atributos para generar un modelo de predicción con un score aceptable para el problema concreto.

En este estudio empírico se pudo comprobar que para el caso del dataset CICIDS2017, en el cual se seleccionaron solo los ataques Dos/DDos, es posible obtener un subconjunto de características que permita mantener los resultados de desempeño muy similares al obtenido con el total de atributos, pero reduciendo notablemente el tiempo de ejecución.

El resultado de este trabajo puede verse como un aporte en ciberseguridad abriendo caminos para explorar con mayor detalle los efectos de la sintonización de los algoritmos de ML en la predicción de ataques Dos/DDos y probar si estos hallazgos se mantienen en los modelos en producción con tráfico en tiempo real.

Quedan como trabajos futuros enfrentar estos espacios planteados y evaluar el comportamiento con otros algoritmos, en particular con enfoques de boosting y de aprendizaje profundo. Además, ver si se puede generalizar a otros tipos de ataques.

AGRADECIMIENTOS

Este trabajo se llevó a cabo en el marco del Proyecto *Prototipo para detección de ataques de DDoS basado en aprendizaje de máquina en una arquitectura orientada a servicios en la nube*, con código 54308; aprobado en el marco de la Convocatoria Conjunta de investigación, desarrollo tecnológico e innovación – 2020, de la Universidad Nacional de Colombia y Universidad de Caldas.

REFERENCIAS

Bramer, M. Principles of Data Mining. 2013 https://doi.org/10.1007/978-1-4471-4884-5.

Chaudhary, A., & Shrimal, G. (2019). Intrusion Detection System Based on Genetic Algorithm for Detection of Distribution Denial of Service Attacks in MANETs. SSRN Electronic Journal, 370–377. https://doi.org/10.2139/ssrn.3351807

Dong, S., Su, H., & Liu, Y. (2022). A-CAVE: Network abnormal traffic detection algorithm based on variational autoencoder. ICT Express. https://doi.org/10.1016/j.icte.2022.11.006

Hadeel S. Obaid. (2020). Denial of Service Attacks: Tools and Categories. International Journal of Engineering Research And, V9(03), 631–636. https://doi.org/10.17577/ijertv9is030289

Hua, Y. An Efficient Traffic Classification Scheme Using Embedded Feature Selection and LightGBM. 2020.

Humayun, M., Niazi, M., Jhanjhi, N., Alshayeb, M., & Mahmood, S. (2020). Cyber Security Threats and Vulnerabilities: A Systematic Mapping Study. Arabian Journal for Science and Engineering, 45(4), 3171–3189. https://doi.org/10.1007/s13369-019-04319-2

Iram, A. Zahrah, A., Faheem, M. and Alwi M, A Machine Learning Approach for Intrusion Detection System on NSL-KDD Dataset. 2020.

Lee, T. H., Chang, L. H., & Syu, C. W. (2020). Deep learning enabled intrusion detection and prevention system over SDN networks. 2020 IEEE International Conference on Communications Workshops, ICC Workshops 2020 - Proceedings. https://doi.org/10.1109/ICCWorkshops49005.2020.9145085

Mahmood, R., Abdi, A. and Hussin, M. “Performance evaluation of intrusion detection system using selected features and machine learning classifiers,” Baghdad Science Journal, vol. 18, pp. 884–898, Jun. 2021, doi: 10.21123/bsj.2021.18.2(Suppl.).0884.

Manso, P., Moura, J., & Serrão, C. (2019). SDN-based intrusion detection system for early detection and mitigation of DDoS attacks. Information (Switzerland), 10(3), 1–17. https://doi.org/10.3390/info10030106.

Montes, A. Isaza, G., Arango, J., Duque-Méndez, N., Ramirez, F. Selection of features in the performance of IDS based on machine learning. 2023.

Muraleedharan, N., & Janet, B. (2021). A deep learning based HTTP slow DoS classification approach using flow data. ICT Express, 7(2), 210–214. https://doi.org/10.1016/j.icte.2020.08.005.

Nazir, A. and Khan, R. “A novel combinatorial optimization based feature selection method for network intrusion detection,” Comput Secur, vol. 102, Mar. 2021, doi: 10.1016/j.cose.2020.102164.

Ortiz Martínez, E. Arguijo, Hiram, P. Vázquez López, R., and Armenta, M. “Selección de características con método wrapper para un sistema de detección de intruso: caso CICIDS-2017 Feature Selection with a Wrapper Method for Intrusion Detection System: Case CICIDS-2017,” 2020.

Panigrahi, R., & Borah, S. (2018). A detailed analysis of CICIDS2017 dataset for designing Intrusion Detection Systems Analysis of Selected Clustering Algorithms Used in Intrusion Detection Systems View project IEEE International Conference on Advanced Computational and Communication Paradigms (ICACCP-2017) View project A detailed analysis of CICIDS2017 dataset for designing Intrusion Detection Systems. In Article in International Journal of Engineering & Technology (Vol. 7, Issue 3). https://www.researchgate.net/publication/329045441

Quiroz, & Valencia, D. (2017). Seguridad en informática: consideraciones. Dominio de Las Ciencias, 3(3), 676–688.

Russell, R. Machine Learning Step-by-Step Guide To Implement Machine Learning Algorithms with Python. (2018. https://books.google.com/books?id=9O-mtwEACAAJ

Sallam, A. A., Kabir, M. N., Alginahi, Y. M., Jamal, A., & Esmeel, T. K. (2020). IDS for Improving DDoS Attack Recognition Based on Attack Profiles and Network Traffic Features. Proceedings - 2020 16th IEEE International Colloquium on Signal Processing and Its Applications, CSPA 2020, Cspa, 255–260. https://doi.org/10.1109/CSPA48992.2020.9068679