e-ISSN: 2528-8091
Vol. 7, N° 3 - 2022

Seguridad contra ataques DDoS en los entornos SDN con Inteligencia Artificial

Security against DDoS attacks in SDN environments with Artificial Intelligence

DOI: *https://doi.org/10.33262/rmc.v7i3.2844*

José Teodoro Mejía Viteri[1]
Universidad Técnica de Babahoyo, Ecuador
https://orcid.org/0000-002-4764-778X
jmejia@utb.edu.ec

María Isabel Gonzales Valero[2]
Universidad Técnica de Babahoyo, Ecuador
https://orcid.org/0000-0001-5825-0668
mgonzalez@utb.edu.ec

Ana del Rocío Fernández Torres[3]
Universidad Técnica de Babahoyo, Ecuador
https://orcid.org/0000-000
afernandez@utb.edu.ec

Narcisa María Crespo Torres[4]
Universidad Técnica de Babahoyo, Ecuador
https://orcid.org/0000-0002-0385-180X
ncrespo@utb.edu.ec

RESUMEN

Las redes definidas por software (SDN), representan la innovación, porque combinan la administración central y la capacidad de programar la red, SDN centraliza la gestión a través de un controlador , separa el plano de control y el datos, pero al tener un único punto de control la hace vulnerable especialmente a los ataques de Denegación de Servicio Distribuido(DDoS), en la actualidad existe muchas investigaciones orientadas a mitigar este tipo de ataques a través de técnicas donde interviene la inteligencia artificial y sus diversas áreas. Este estudio describe las SDN, la inteligencia artificial, los ataques

e-ISSN: 2528-8091
Vol. 7, N° 3 - 2022

DDoS y realiza una revisión de la intervención de la inteligencia artificial para mitigar este tipo de ataques.

Palabras clave: *DN, DDoS, Inteligencia Artificial, Algoritmos de Aprendizaje.*

ABSTRACT.

Software-defined networks (SDN) represent innovation, because they combine central administration and the ability to program the network, SDN centralizes management through a controller, separates the control plane and the data, but having a single Control point makes it especially vulnerable to Distributed Denial of Service (DDoS) attacks, currently there are many investigations aimed at mitigating this type of attack through techniques where artificial intelligence and its various areas intervene. This study describes SDN, artificial intelligence, and DDoS attacks and reviews the intervention of artificial intelligence to mitigate these types of attacks.

Palabras clave: *DN, DDoS, Artificial Intelligence, Learning Algorithms*

INTRODUCCIÓN

Las redes definidas por software (SDN) **,** proporcionan servicios fiables y suficientes basados en un tipo de tráfico especifico, porque mantienen una vista global de los estados de red y proporciona control de nivel de flujo de cada una de las capas que la conforman, el paradigma .SDN separa el plano de datos del plano de control, dando como resultado un enfoque más rápido y dinámico en comparación con un red convencional.

SDN tiene un controlador lógicamente centralizado que puede analizar el tráfico y configurar nuevas instrucciones para ser enviadas a las tablas de los conmutadores, se puede definir como el cerebro de la red porque gestiona todos los flujos de tráfico de la red; toma decisiones basadas en el análisis de los flujos de tráfico y recopila estadísticas de paquetes entrantes (Aladaileh et al. 2020), esta capacidad permite a SDN descubrir y reaccionar ante anomalías de la red, el desacoplamiento del plano de control de la red del de datos abre una ventana para los atacantes exploten y cree una vulnerabilidad de seguridad(Jiang et al. 2018), todo esto convierte al controlador en un punto único de riesgo de falla y podría afectar el rendimiento de la red, la disponibilidad y por tanto la confiabilidad, los ataques DDoS son una amenaza para la estabilidad de la red, estos ataques por lo general provienen de múltiples fuentes y distribuidos geográficamente, suele iniciar escaneando la red para encontrar la vulnerabilidad, posteriormente busca infectar host vulnerables para obtener el control a través de programas maliciosos e

e-ISSN: 2528-8091
Vol. 7, N° 3 - 2022

intentan evitar que los usuarios legítimos accedan a los recursos de la red o denegar los accesos a los servicios de la red(Yan et al.2016), los atacantes continuamente cambian los métodos de estos ataques representando una serie amenaza especialmente si afecta el controlador SDN sin embargo, proteger el controlador SDN del ataque DDoS es una tarea desafiante y que consume muchos recursos que reduce la efectividad del controlador en la gestión de la red. Esto es aún más dado que existen diferentes tipos de ataques DDoS en SDN , esto indica que cualquier esfuerzo para proteger la infraestructura de una SDN contra los ataques DDoS requiere de una comprensión de las características de SDN, tráfico y los ataques DDoS con sus comportamientos para encontrar patrones que se podrían usar como indicadores para detección de este tipo de ataques.

Las contribuciones de este documento son: comprender el funcionamiento de un ataque DDoS y como estos pueden afectar al controlador SDN, revisar diferentes campos de la Inteligencia Artificial para comprender su funcionamiento y establecer como ayudan a la identificación de los ataques DDoS, hacer una revisión las diferentes técnicas de detección a través de los campos de la inteligencia artificial.

MATERIALES Y MÉTODOS.

Para dar cumplimiento al objetivo del estudio que es realizar un estado del arte en cuanto a las técnicas utilizadas en la detección de los ataques DDos con Inteligencia Artificial en entornos de Redes definidas por software (SDN) en su siglas en inglés, para esto se realizo un búsqueda bibliográfica en las diferentes base de datos internacionales como Scopus y Springer IEEE y otras, que reúnen investigaciones relacionadas con el tema y evidencian resultados, y presentan ideas y técnicas de forma clara, y crear una base de datos teórica con un enfoque documental estándar bibliográfico.

La búsqueda se enfocó en los siguientes temas:

1.- Redes definidas por Software (SDN), especialmente sobre estructura, funcionamiento.

2.- Diferentes áreas de la inteligencia artificial.

3.- Ataques de Denegación de Servicio Distribuido
(DDoS).

4.- Estudios de cómo combatir los ataques DDoS en los entornos SDN con las diferentes áreas de la inteligencia artificial.

e-ISSN: 2528-8091
Vol. 7, N° 3 - 2022

DESARROLLO.

SDN, promueve la innovación porque introduce el concepto de programabilidad en el plano de datos. La arquitectura de SDN es diseñado en la separación por capas del plano de control y de datos. En la figura 1 se muestra como se estructura.

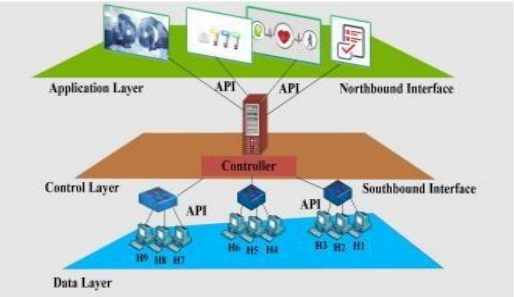

Fig 2: Estructura SDN Fuente: (Mohammad, 2020)

Esta división de los planos de control y datos aportan flexibilidad a la hora de definir políticas de red, ejecutarlas en conmutadores y enrutadores y luego impulsar el reenvío de tráfico e introduce nuevas abstracciones de tráfico que rompen el problema relacionado con el control de la red en pequeños fragmentos(Kim & Suk ,2016).

La aparición de SDN, desde el punto de vista global, evita la limitación del hardware en la arquitectura de la red, reduce el costo de administración de la red y operación. SDN presenta un controlador como el cerebro de toda la red, este es responsable de todo el control de la red, y la lógica de control es supervisada por el plano de control, esto produce que la gestión de la red sea más conveniente. También existe una gran mejora en la eficiencia de la operación, el mantenimiento y la gestión de la red (Xiaoqiong, Hongfang, & Kun,2017).

Las aplicaciones de SDN residen en el plano de aplicación de la arquitectura SDN donde la interfaz de programación de aplicaciones (API) de northbound proporciona la conmutación entre los planos de aplicación y control, esto permite implementar un conjunto de servicios de red, detección de intrusiones, calidad de servicio, corta fuego y monitoreo (Latah Toker,2019),estas API northbound permiten a los desarrolladores realizar aplicaciones sin necesidad de un conocimiento detallado del controlador o del funcionamiento del plano de datos. La comunicación entre los planos de control y de datos se proporciona mediante una API southbound, como el reenvío y la separación de elementos de control (ForCES) , la base de datos v Switch abierta (OVSDB), protocolos

e-ISSN: 2528-8091
Vol. 7, N° 3 - 2022

como (POF) , OpenState , OpenFlow (OF) y OpFlex , que permite intercambiar mensajes de control .

Open Flow

OpenFlow (OF) se considera la API south-bound más utilizada en SDN, que está siendo desarrollada y estandarizada continuamente por Open Network Foundation (ONF) [6]. OF proporciona una capa de abstracción que permite al controlador SDN comunicarse de forma segura con elementos de reenvío habilitados para OF (Nunes et al. 2014).

Los dispositivos de reenvío basados en OF se han desarrollado para coexistir con dispositivos Ethernet convencionales (Kreutz , 2015). Los conmutadores híbridos, por otro lado, revelan nuevas posibilidades al incluir puertos OF y no OF. El controlador puede enviar un conjunto de mensajes de control para preparar y actualizar las tablas de flujo de un conmutador en particular. Un conmutador habilitado para OF típico maneja los nuevos paquetes que vienen en función de su tabla de flujo. La figura 2 muestra los campos de la parte de reglas de coincidencia en OF versión 1.0. Un error de tabla ocurre cuando un nuevo paquete no coincide con ninguna de las entradas de la tabla de flujo. En este caso, el conmutador puede descartar el paquete o reenviarlo al controlador correspondiente utilizando el protocolo OF(Nunes et al. 2014).

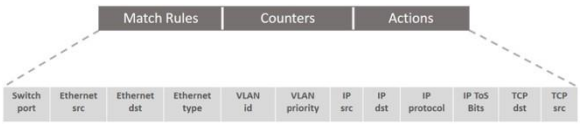

Fig. 1. Parte de reglas de coincidencia.
Fuente:(Latah, Majd, &Levent Toker. 2019)

La inteligencia Artificial es una área de conocimiento que tiene muchas subáreas, incluida la representación del conocimiento, la toma de decisiones, aprendizaje automático(ML) y los algoritmos metaheurísticos (Latah & Toker 2019). La investigación de la Inteligencia artificial inició en la década de 1950 a través en un taller dirigido por Martín Minsky y Calude Shannon en Dourmouth College que dio origen a la IA(Negnevitsky, 2005), se conoce también que la primera contribución fue hecha en 1943 por McCulloch y Pitts que propusieron el modelo de redes neuronales, donde esas neuronas tiene una salida binaria +1 y -1con una función de activación de signo(Negnevitsky , 2005), posteriormente aparecieron otros enfoques provocando que existan otra sub-áreas, como los sistemas expertos, lógica difusa, computación evolutiva

e-ISSN: 2528-8091
Vol. 7, N° 3 - 2022

y otras, todo este esfuerzo impulsó a perfeccionar los métodos existentes y proponer nuevos enfoques. En la actualidad el aprendizaje automático, los sistemas de inferencia difusa se utilizan ampliamente en SDN, razón por la cual los diversos enfoques serán detallados a continuación.

Aprendizaje Automático. Es el aprendizaje que se obtiene de la experiencia de los datos obtenidos de su entorno(Russell & Norvig, 1995), en este contexto se divide en 4 grupos.

Aprendizaje Supervisado. Este método proporciona un conocimiento predefinido por ejemplo, un conjunto de datos de entrenamiento que consta de pares de entrada-salida, donde el sistema aprende en función que asigna una entrada dada una salida apropiada.(Russell & Norvig 1995).

Redes neuronales artificiales. Ofrece medios para modelar de manera efectiva y eficiente problema grandes y complejos. Los modelos de ANN son dirigidos a partir de datos, es decir, son capaces de encontrar relaciones (patrones de forma inductiva por medio de algoritmos de aprendizaje basado en datos existentes(Salas,2017).

Máquinas vectores de soporte. Son un tipo de red neuronal que fue originalmente diseñado para la solución de problemas no lineales de clasificación que recientemente se aplican a problemas de regresión y predicción de series temporales.(Velásquez, Olaya, & Franco, 2010).

Árboles de decisión. Un árbol de decisión es un modelo de predicción cuyo objetivo principal es el aprendizaje inductivo a partir de observaciones y construcciones lógicas. Son muy similares a los sistemas de predicción basados en reglas que sirven para representar y categorizar una serie de condiciones que suceden de forma sucesiva para la solución de un problema(Martínez, 2009).

Métodos de conjunto. Los métodos de conjunto combinan predicciones de diferentes enfoques (mediante votación ponderada o no ponderada) y se utilizan para mejorar el rendimiento de los algoritmos de aprendizaje(Russell & Norvig, 1995).

Aprendizaje profundo. El primer precedente en el uso exitoso del aprendizaje profundo se debe a Geoffrey Hinton quien introdujo las redes de creencia profunda utilizando una capa de red una Máquina de Boltzmann restringida(RBM) para asignación inicial de pesos sinápticos.

Estos modelos consisten en técnicas de aprendizaje supervisado o no supervisado teniendo como estructura principal varias capas de redes neuronales artificiales que son capaces de aprender una representación jerárquica en arquitecturas profundas. Las arquitecturas de aprendizaje profundo están compuestas de varias capas de

e-ISSN: 2528-8091
Vol. 7, N° 3 - 2022

procesamiento, donde cada capa produce respuestas no-lineales basadas en la capa anterior y la entrada inicial(López & Ramos, 2019).

Redes Neuronales Recurrentes. Son sistemas dinámicos, el cálculo de una entrada en un paso, depende del paso anterior y en algunos casos del paso futuro, estas redes RnR son capaces de realizar una amplia variedad de tareas computacionales incluyendo el tratamiento de secuencias, la continuación de una trayectoria, la predicción no lineal y la modelación de sistemas dinámicos(Cruz, Martinez, & Abed, 2007).

Redes neuronales convolucionales. Esta redes neuronales son un tipo particular de red neuronal inspirada en el funcionamiento de la corteza visual del cerebro, están diseñadas para resolver problemas de visión artificial como el reconocimiento de patrones, aunque pueden tener otros usos como la clasificación de textos o el procesamiento de lenguaje natural(Sánchez,2016).

Aprendizaje no supervisado. En este tipo de aprendizaje los algoritmos trabajan de forma parecida a los supervisados, con la diferencia de que estos solo ajustan su módulo predictivo a través de la toma de datos de entrada, dejando de lado los datos de salida, en otras palabras, a diferencia del supervisado, los datos correspondiente a la entrada no se encuentran clasificados ni etiquetados, por lo que son necesarias estas características para entrenar el modelo.

Agrupación de K-means. En el algoritmo de agrupamiento de mayor popularidad en el campo de la gestión de repositorios de modelos de BPs es el K-means, debido a su simplicidad y rendimiento. Este algoritmo es no supervisado y se usa comúnmente para agrupar elementos como documentos de texto, documentos web, imágenes, modelos de BPs, entre otros tipos de datos (Ordoñez,Cobos,Torres & Buchelly, 2019).

Mapas autooroganizados. Entre los clasificadores no supervisados uno de los modelos más extendidos son los mapas autoorganizados (SOM), el algoritmo del SOM realiza la transformación de un espacio de entrada de dimensión alta a otro de dimensión más baja (usualmente bidimensional o tridimensional) formado por una red regular de nodos. El proceso se realiza preservando la topología inicial del espacio de entrada (Cortada & Sanromà, 2003).

Modelo de Markov oculto (HMM). En los sistemas de clasificación basados en HMM, la identificación de las clases se suele realizar caracterizando las señales como una secuencia de vectores de características y entrenando por cada clase un modelo oculto de Markov. Para una nueva observación, por cada HMM se calcula la verosimilitud y el

e-ISSN: 2528-8091
Vol. 7, N° 3 - 2022

modelo que entregue la verosimilitud mayor se escoge como el modelo que representa la clase correcta.

Máquina de Boltzmann restringida *(RBM)***.** Las máquinas restringidas de Boltzmann (RBM) son caracterizadas por su topología o estructura bipartida(Desjardins, 2010). Poseen enlaces únicamente entre las unidades ocultas y visibles pero no entre unidades de una misma capa, y por tanto no existen dependencias entre nodos visibles o entre nodos oculto(Tosun,2014).

Enfoques de aprendizaje profundo no supervisados. Como mencionamos anteriormente, las arquitecturas profundas se clasifican en:

1) modelos generativos,
2) discriminativos y
3) híbridos

También mencionamos que los modelos generativos emplean enfoques de aprendizaje no supervisados para caracterizar las propiedades de correlación de orden superior de los datos de entrada. Los modelos generativos necesitan una etapa de pre entrenamiento sin supervisión para extraer las estructuras en los datos de entrada. También necesitan una capa superior adicional para realizar la tarea discriminativa(Deng ,2014).

Los codificadores automáticos (AE) son adecuados para la extracción de características y la dimensionalidad de la reducción. Un codificador automático básico tiene dos etapas:

1) codificación
2) etapa de decodificación

El primer escenario recibe los datos de entrada y los transforma en una nueva representación, llamado código o variable latente, mientras que la segunda etapa recibe el código generado en la primera etapa y reconstruye el dato de entrada original. El procedimiento de formación tiene como objetivo minimizar el error de reconstrucción(Mohammadi, 2018).

Redes de creencia profunda. Geoffrey Hinton demostró que las RBMs pueden ser apiladas y entrenadas de una manera egoísta para formar lo que el denominó redes de creencia profunda (DBN). Las redes de creencia profundas son modelos gráficos que aprenden a extraer una representación jerárquica profunda de los datos de entrenamiento(Hinton, Osindero & Teh ,2006).

e-ISSN: 2528-8091
Vol. 7, N° 3 - 2022

M. Aprendizaje por refuerzo. El aprendizaje por refuerzo, RL (Reinforcement learning), consiste en mapear situaciones a acciones maximizando un escalar denominado señal de refuerzo o recompensa. Es una técnica de aprendizaje basada en prueba y error. El aprendizaje por refuerzo se utiliza cuando no existe una información detallada sobre la salida deseada, por el contrario del aprendizaje supervisado, no existe un maestro que permita indicar las salidas correctas ante determinadas entradas.

N. Q-learning. ***El Q-learning*** es uno de los algoritmos de aprendizaje por refuerzo más importantes y fue presentado por Watkins en 1989 este algoritmo es una combinación de la programación dinámica, más concretamente el algoritmo de Iteración de Valores y la aproximación estocástica. Se considera un método que involucra el concepto de "modelo libre de aprendizaje por refuerzo", esto quiere decir que se proporciona al agente con la capacidad de aprender, para actuar en un dominio Markoviano por la experiencia dada por la consecuencia de acciones(Guo, Liu, & Malec,2004).

Algoritmos metaheurísticos. Son algoritmos aproximados de optimización y búsqueda de propósito general. Son procedimientos iterativos que guían una heurística subordinada combinando de forma inteligente distintos conceptos para explorar y explotar adecuadamente el espacio de búsqueda(Herrera, 2015).

Optimización de colonias de hormigas. Los algoritmos ACO (Ant Colony Optimization) son modelos inspirados en el comportamiento de colonias de hormigas reales. Estudios realizados explican cómo animales casi ciegos, como son las hormigas, son capaces de seguir la ruta más corta en su camino de ida y vuelta entre la colonia y una fuente de abastecimiento(Barcos, 2002).

Algoritmos evolutivos. Los algoritmos evolutivos son métodos robustos de búsqueda, que permiten tratar problemas de optimización donde el objetivo es encontrar un conjunto de parámetros que minimizan o maximizan una función de adaptación (Valencia, 2014.).

Algoritmo Genético. Más formalmente, y siguiendo la definición dada por Goldberg, "los Algoritmos Genéticos, son algoritmos de búsqueda basados en la mecánica de selección natural y de la genética natural. Combinan la supervivencia del más apto entre estructuras de secuencias con un intercambio de información estructurado, aunque aleatorizado, para constituir así un algoritmo de búsqueda que tenga algo de las genialidades de las búsquedas humanas(Gestal, 2010).

e-ISSN: 2528-8091
Vol. 7, N° 3 - 2022

Optimización de Enjambre de Partículas. La metaheurística de Optimización de Enjambre de Partículas o PSO por sus siglas en inglés (Particle Swarm Optimization), fue desarrollada por Kennedy y Eberhart [Kennedy95] y está inspirada en el comportamiento social observado en grupos de individuos tales como parvadas de pájaros, enjambres de insectos y bancos de peces(Lima & Barán, 2006).

Recocido Simulado. Recocido simulado es una metaheurística popular usada para resolver problemas discretos y continuos. La metaheurística recocido simulado adopta su nombre gracias a la analogía con el proceso físico de recocido con sólidos, la principal característica de la metaheurística de recocido simulado es que proporciona una alternativa eficiente para escapar de óptimos locales al permitir movimientos "peores" respecto a la función objetivo (hill-climbing moves) en aras de encontrar un óptimo global(Escobar & Linfati, 2012).

Algoritmo de la colonia artificial de abejas (ABC).

El algoritmo de la colonia artificial de abejas (ABC) es uno de los algoritmos más recientes en el dominio de la inteligencia colectiva. Fue propuesto por Dervis Karaboga en 2005 [17] está basado en el comportamiento de forrajeo de las abejas, y diseñado originalmente para problemas de optimización numérica, aunque puede ser utilizado para resolver problemas de combinatoria(García s. f.).

Algoritmo de murciélagos (BA). Este algoritmo propuesto por Yang utiliza las características de ecolocalización de los murciélagos. Se basa en las siguientes reglas: (1) Todos los murciélagos usan ecolocalización para medir la distancia, y ellos "saben" de alguna manera la diferencia entre comida/presa y los límites de búsqueda.

(2) Los murciélagos vuelan aleatoriamente con velocidad

vi en la posición xi con una frecuencia fija fmin, variando la longitud de onda λ y la intensidad A0 para buscar a su presa, Aunque la intensidad puede variar de muchas formas , asumimos que varía desde una gran (positivo) A0 a un valor mínimo constante Amin(Velásquez & Candoti,2015) .

Sistema de Inferencia Difusa. Un Sistema de Inferencia Difuso – FIS, es una forma de representar conocimientos y datos inexactos en forma similar a como lo hace el pensamiento humano. Un FIS define una correspondencia no lineal entre una o varias variables de entrada y una variable de salida; esto proporciona una base desde la cual pueden tomarse decisiones o definir patrones(Hurtado & Gómez, 2008).

e-ISSN: 2528-8091
Vol. 7, N° 3 - 2022

Después de analizar los diversos campos de la inteligencia artificial se procede en el análisis de los ataques DDoS, su conceptualización y sus variantes y funcionamiento en las redes SDN.

Los ataques DDoS descripción y funcionamiento. El diseño del entorno SDN que desacopla el plano de control del plano de datos permite soluciones de seguridad innovadoras para proteger las redes de los ataques. Permite que la red para ser administrada dinámicamente a través de una función de control lógica y centralizada que proporciona instrucciones al plano de datos para reenviar el tráfico de la red(Kreutz, Ramos, & Verissimo,2013), esta función de control centralizado de la red es una desventaja porque se convierte en el objetivo principal de una atacante debido a la dependencia de toda la red de este controlador.

Los ataques de Denegación de servicio distribuido DDoS es una amenaza que afecta a la estabilidad de la red, esto a la enorme asimetría de recursos entre la red y la víctima, estos ataques no vienen de una sola fuente sino de múltiples además de estar distribuidos en diferentes ubicaciones geográficas.

Los ataques de denegación de servicio (DoS) buscan
restringir parcialmente o negar completamente el acceso de usuarios legítimos a los recursos proporcionados por la red, computadora o servicio de la víctima. Cuando este intento se inicia desde un solo host, el ataque se llama un ataque DoS. Si bien los ataques DoS se pueden montar con éxito usando un solo host con recursos limitados, la mayoría de los ataques requieren un grupo de hosts maliciosos conocidos como “bots” que inundan la red de la víctima con una cantidad abrumadora de paquetes de ataques. Este tipo de ataque se denomina denegación de servicio distribuido (DDoS)(Martínez & Ortiz 2019).

El principal objetivo del ataque DDoS dirigido al controlador SDN es abrumar y agotar sus recursos, normalmente inundando la red con paquetes IP falsificados, lo que genera una congestión que degrada o colapsa la red (Kreutz. 2013). Existen varias características de los ataques DDoS a las redes SDN, a continuación, se detallan.

- Los atacantes forjan enlaces entre conmutadores, provocan fallas en el enlace e inhibe la comunicación rápida, existe sobrecarga de la tabla de flujo.
- Los atacantes utilizan la teoría del juego, un atacante apunta a un nodo para ser atacado en la red durante un periodo de salto los atacantes comprometen los nodos legítimos.

e-ISSN: 2528-8091
Vol. 7, N° 3 - 2022

- Los atacantes generalmente abruman la tabla de conmutación al inundar la red con paquetes IP falsificados hasta que la tasa de llegada de paquetes entrantes está más allá de la capacidad de manejo del controlador y se agotan sus recursos. Por lo tanto, el controlador SDN centralizado se convierte en un único punto de falla en tal situación.
- Un atacante usa los conmutadores OpenFlow para abrumar al controlador con una gran cantidad de paquetes en lugar de atacar al controlador directamente, ya que los paquetes entrantes se reenviarán automáticamente al controlador para su procesamiento.
- El controlador es responsable de actualizar las reglas de flujo y configurar nuevas reglas de acuerdo con el flujo. Sin embargo, los atacantes podrían aprovechar la brecha en el tiempo de reacción del controlador al manejar nuevos paquetes de red para lanzar su ataque al controlador SDN enviando una gran cantidad de solicitudes al controlador dentro de esta ventana de tiempo.
- Los ataques DDoS suelen utilizar el mismo tamaño de paquete medio. Dado que el tráfico de ataque tiene una alta tasa de bits, el tiempo para llegar a la máquina objetivo es muy corto. Los atacantes se centran en cualquiera de estas funciones para consumir los recursos de la máquina objetivo y evitar que funcione.

Estas son algunas de las principales características descritas en varios trabajos de investigación, sin embargo, estos enfoques son incapaces de detectar ataques DDoS que cambian continuamente sus comportamientos de ataque, debido a la dependencia de las reglas de conmutación estáticas. Las reglas de conmutación estáticas o las tablas de flujo de conmutación no son efectivas para tratar con atacantes que siguen cambiando el comportamiento del tráfico de ataque para que se parezca al tráfico normal (Aladaileh,2020).

- En la actualidad las técnicas para combatir los ataques de DDoS utilizan la inteligencia artificial a continuación, se detallan algunas de las soluciones que varios investigadores realizaron para evitar ser vulnerables por este tipo de ataque

DISCUSIÓN Y RESULTADOS

Los estudios analizados sobre detección de tráfico de ataques DDos utilizando inteligencia artificial, establecen los autores la descripción de la técnica y el área de

e-ISSN: 2528-8091
Vol. 7, N° 3 - 2022

inteligencia artificial que se utiliza, en lo trabajos los investigadores utilizan datos púbicos que tienen el tráfico de red de topologías de red como KDD Cup'99,NSL-KDD,UNB-Iscx,CICIDS2017 y CAIDA 2016, utilizar estos tráficos es bueno para el entrenamiento de los algoritmos utilizados, sin embargo todas las infraestructuras SDN no son iguales, por tanto se pueden desarrollar nuevos vectores de ataques , por estos algoritmos se deben someter a continuas pruebas y con datos actualizados.

Este trabajo desarrolla una perspectiva teórica, contribuyen haciendo conocer las diferentes áreas de la inteligencia artificial y revisar los ataques DDoS, para establecer patrones y revisar el estado del arte de como están ayudando las diferentes áreas de la inteligencia artificial a detectar este tipo de ataques e implementar soluciones que no consuman los recursos de la red y permitan proteger al controlador SDN que es su principal objetivo.

Técnicas de detección de los ataques DDoS basadas en la inteligencia artificial.

Los investigadores en la actualidad están realizando grandes esfuerzos para integrar la Inteligencia Artificial en SDN, en esta sección se centra en establecer una visión del papel de la IA en la seguridad para detección de los ataques DDoS.

Arquitectura SDNmulticontroller.

Esta Arquitectura utiliza un clasificador difuso con L1-Extreme Learning Machine (L1-ELM)). Para lograr un procesamiento más rápido, este clasificador híbrido se ejecuta a través de una red neuronal.

Los conmutadores evalúan a cada usuario en el flujo utilizando una confianza valor. El valor de confianza es un campo adicional que se incluye junto con la tabla de flujo del usuario y su valor depende del intercambio de datos de cada usuario.

Para hacer esto, el clasificador primero extrae varias características de los paquetes de flujo de los hosts. El sistema de lógica difusa considera tres características importantes: la dirección IP de origen, el número de puerto de origen y el número de puerto de destino. Los números de puerto almacenados en el repositorio del controlador proporciona el soporte inicial para detectar anomalías. El sistema de lógica difusa se aplica como una verificación usando estas tres características del paquete.

Las características de los paquetes se clasifican de forma amplia como básico, basado en contenido, basado en tiempo y basado en conexión características para el sistema difuso, las tres características básicas se consideran de tipo "continuo".

e-ISSN: 2528-8091
Vol. 7, N° 3 - 2022

Las características del paquete juegan un papel importante en la detección y mitigar los tres tipos de ataques. Los resultados de la clasificación distinguir los paquetes normales de los paquetes anómalos(Abdulqadder,2018).

Algoritmo SVM (Self Organizing Maps).

Se utiliza para distinguir entre tráfico normal y tráfico anormal de un ataque, consiste principalmente de la colección de estado de flujo, la principal característica de extracción valores, y el juicio del clasificador, la recopilación del estado de flujo envía periódicamente una solicitud a la tabla de flujo a el switch Open Flow y envía información a la tabla de flujo respondiendo desde el switch a la colección de estados de flujo.

La extracción de valores característicos es la responsable de extraer los valores característicos relacionados con el ataque DDoS de la tabla de flujo del switch y componiendo la matriz six- tuple de valores característicos se clasifica mediante el uso de un algoritmo basado en SVM para distinguir entre tráfico normal y ataque tráfico anormal(Ye, 2018).

Aprendizaje automático y NCA(Neighbourhood Component Analysis

En este estudio, el tráfico normal y de ataque en el conjunto de datos obtenido del entorno SDN se clasificó mediante algoritmos de aprendizaje automático. El conjunto de datos consta de tráfico normal y de ataque TCP, UDP e ICMP. El conjunto de datos tiene características estadísticas como byte_count, duration_sec, velocidad de paquete y paquete por flujo, excepto para las funciones que definen las máquinas de origen y de destino. El algoritmo NCA se ha utilizado para realizar una clasificación eficaz y seleccionar las características más adecuadas. Después de analizar 22 características de red algoritmos NCA, se seleccionaro 14 características efectivas y se proporcionaron como entrada a los algoritmos de aprendizaje automático.

Para garantizar un modelo híbrido ligero equipado con enfoques de aprendizaje automático y NCA(Neighbourhood Component Analysis), para detectar ataques DDoS con aprendizaje automático, algunos características del flujo (tamaño del paquete, tiempo de llegada, tiempo de respuesta, velocidad de paquete, paquete por flujo, etc.) se utilizan para identificar si el tráfico de la red es normal, los ataques DDoS suelen utilizar mismo tamaño de paquete promedio, garantizar un modelo híbrido ligero equipado con enfoques de aprendizaje automático y NCA(Neighbourhood Component Analysis).

Dado que el tráfico de ataque tiene una tasa de bits alta, el tiempo para llegar a la máquina de destino es muy corta Para ello, manejamos un conjunto de datos público (Data set) que

e-ISSN: 2528-8091
Vol. 7, N° 3 - 2022

incluye un total de 23 funciones para detectar ataques DDoS con aprendizaje automático.En lugar de considerar todas las características del conjunto de datos, revelamos las características más eficientes con el enfoque NCA con la ayuda del modelo recientemente propuesto(Tonkal et al. 2021).

RNN(Recurrent Neural Networks).

Usa una técnica híbrida que comprende la red neuronal Cuda-Deep Memoria a corto plazo (CuDNNLSTM) y Cuda-Deep Neural Network Gated Algoritmos de unidad recurrente (CuDNNGRU) para una amenaza eficiente También implementamos dos algoritmos para la comparación de nuestra detección de resultados: Cuda- Deep Neural Network Unidad recurrente cerrada (CuDNN-GRU) y memoria a corto plazo Cuda- bidireccional a largo plazo (CuBLSTM).

Una técnica híbrida de aprendizaje profundo para la detección eficiente de amenazas en un entorno de IoT que comprende ANN basado en MLP se utiliza para construir límite de decisión de clasificación en el espacio de características para realizar como función discriminadora no lineal.

En paquetes basados en NN sistema de clasificación, cada elemento del vector de características tiene un nodo de entrada.

Además, normalmente se utiliza un nodo de salida para cada clase a la que se le puede asignar una característica

Los nodos ocultos están conectados a los nodos de entrada y algún peso inicial asignado a estas conexiones. Estos pesos se ajustan durante el proceso de formación Propagación hacia atrás (Back Propagation)

La regla es uno de los algoritmos de aprendizaje utilizados para MLP.

La regla de propagación ANN funciona en un método de descenso de gradiente este método calculó una función de error que es la diferencia entre la salida calculada por la red y la salida deseada. El error cuadrático medio (MSE) se utiliza para defina esta función de error. El MSE se agrega sobre el conjunto de entrenamiento completo. Para aprender con éxito, el verdadero resultado de la red debe acercarse a la salida deseada.

Este es hecho reduciendo el valor de este error, continuamente. para una entrada en particular se calcula mediante (Back Propagation) regla y luego este error se propaga desde una capa a la anterior(Javeed, Gao & Khan 2021).

e-ISSN: 2528-8091
Vol. 7, N° 3 - 2022

ANN(Artificial Network Neural.

El propósito de la detección de intrusiones sistemas basados en NN es clasificar lo normal / válido, y patrones de ataque junto con el tipo de ataque. Por lo tanto, la clasificación de un solo registro se puede hacer fácilmente después de una formación adecuada. Entonces, el IDS basado en NN puede funcionar como un clasificador en línea para el tipo de ataque para el que fue entrenado. El NN estará fuera de línea solo por una pequeña duración cuando está recopilando la información necesaria para calcular las características (Ashraf & Latif, 2014).

DCNN Q-Learning Deep Convolution Neural Network.

En escenarios de ataques LR-DDoS de múltiples objetivos, el ataque fluye casi tienen las mismas características clasificadas con flujos normales, y pueden ser ataques insensibles a objetivos atacados a largo plazo.Como resultado, el método de análisis de volumen de tráfico no puede detectar

un ataque tan sigiloso ya, algunos investigadores presentan los métodos de aprendizaje automático semi-supervisados para detectar ataques LR-DDoS.

Las ventajas son que estos métodos pueden hacer uso de la estructura geométrica subyacente de muestras sin etiquetar para entrenar al clasificador, mientras que las desventajas son que no son adecuado para el aprendizaje incremental y su velocidad de entrenamiento es demasiado lento para cumplir con los requisitos de los usuarios del borde. Para abordar temas anteriores, proponemos una nueva y profunda CNN Q-Network método en este documento.

DCNN puede extraer las funciones disponibles automáticamente, mientras que Q-Network puede ayudar a tomar decisiones y obtenga el control de salida directamente basado en entradas sin procesar por proceso de aprendizaje de principio a fin. Por lo tanto, DCNN Q-Network.El método no solo puede mejorar la precisión de la clasificación detección, pero también acorta el tiempo de procesamiento de la clasificación detección y aliviar eficazmente el ataque LR-DDoS en el borde. DCNN, como modelo de aprendizaje profundo, puede extraer automáticamente características en diferentes niveles, y combinar estas características para producir resultado. Es decir, puede aceptar características de alta dimensión como entradas. Pero las grandes dimensiones y las múltiples capas significan cantidades de parámetros, lo que conduce a un mayor gasto de procesamiento En escenarios de ataques LR-DDoS de múltiples objetivos, el ataque fluye casi tienen las mismas características clasificadas con flujos normales, y pueden ser ataques insensibles a objetivos atacados a largo plazo.

e-ISSN: 2528-8091
Vol. 7, N° 3 - 2022

Como resultado, el método de análisis de volumen de tráfico no puede detectar un ataque tan sigiloso ya. Por lo tanto, diseñamos algunas características sensibles a la localidad para DCNN. La idea de localidad sensible es para resolver el aproximado en espacios de alta dimensión. Puede ayudar a DCNN a mapear elementos similares a los mismos depósitos con alta probabilidad (Liu, Yin, & Hu ,2020).

Som(self-organizing maps)(SVM Support Vector Machine.

Después de recopilar la información de la tabla de flujo, el control SDN extrae el vector de características según al algoritmo de extracción de características y almacena en caché los datos extraídos en tiempo real en un archivo para su almacenamiento. El flujo extraído los vectores de características de la tabla se envían al modelo SVM para su detección. El SVM utiliza la información de vector de características proporcionada para determinar si se trata de tráfico de ataque o tráfico normal. Si es normal tráfico, el resultado se guarda directamente; si se trata de tráfico anormal,se combina con la información de tráfico de la hora anterior después de la estandarización para formar una serie temporal y enviarla al opti-modelo LSTM mized para comprobar. Si el LSTM mod- optimizado el juzga que se trata de tráfico anormal, genera la información de tráfico anormal detectado, lo que indica que está bajo DDoS ataque; si se detecta como tráfico normal, se considera normal tráfico. Además, el método de series de tiempo se utiliza principalmente para Resuelva el problema de las falsas alarmas de un solo tráfico anormal.

Por lo tanto, cuando el clasificador SVM hace un juicio anormal, el sistema enviará la información de la función de la tabla de flujo basada en tiempos anteriores al LSTM profundo optimizado modelo de aprendizaje para emitir un juicio sobre la siguiente información de la tabla de flujo. El resultado final se obtiene mediante el juicio integral del mecanismo de detección.

Nos centraremos en la parte de preprocesamiento de datos, utilizando el algoritmo genético mejorado para optimizar el modelo LSTM e introducir SVM para resolver el problema de juicio erróneo causado por la sensibilidad de los datos LSTM en la etapa inicial de la red (Min, 2020).

K-FKNN(K-means and Fast K-Nearest Neighbors)- BASED DDOS DETECTION SYSTEM

La función de detección de DDoS se implementa como un programa de control. El controlador se comunica periódicamente con el conmutador para recopilar y detectar flujos de red. Si el flujo es detectado como un ataque DDoS, el controlador modificará el flujo de reglas de reenvío de tablas e informar al conmutador de anomalías tratamiento.

e-ISSN: 2528-8091
Vol. 7, N° 3 - 2022

En el plano de control, recolección de flujo de red y preprocesamiento de datos son implementados. El control K-FKNN incluye cuatro módulos: Recopilador de flujo, extractor de funciones, procesador de datos y Base de datos.

Colector de flujo: durante el proceso de detección en tiempo real.

El colector de flujo recopila periódicamente la información del flujo de la red de conmutadores y envía la información a la función Extractor

Extractor de características: extrae características para formar una característica vector del flujo de red. Los datos de la característica incluyen bytes enviados desde el origen al destino, bytes enviados desde el destino a la fuente, tasa de error, etc. Luego, envía el vector a la solicitud de detección.

Base de datos: almacena los datos de entrenamiento, que incluyen datos de ataques DDoS.

Procesador de datos de entrenamiento: normaliza los datos de entrenamiento y emplea el algoritmo K-

meansCC para preprocesar el entrenamiento datos. Los datos de entrenamiento preprocesados serán

explotados por la aplicación de detección de DDoS. La aplicación basada en K-FKNN puede realizar la

detección de DDoS y mitigación. Incluye tres módulos: K-FKNN Initializer, Detector basado en

K-FKNN y mitigación de DDoS.

Inicializador K-FKNN: Establece los valores iniciales de los parámetros requerido en el algoritmo

K-FKNN.

Detector basado en K-FKNN: Después de recibir el vector del flujo de red, normaliza los datos de características del vector y aprovecha el algoritmo K-FKNN y preprocesado datos de entrenamiento para identificar ataques DDoS.

Mitigación de DDoS: si el flujo se detecta como un ataque DDoS, La mitigación de DDoS indicará al controlador que establezca la caída acción en la entrada de flujo de la tabla de flujo. Entonces, el controlador envía la entrada de flujo al conmutador, que eliminará el Flujo malicioso para la protección de la red(Xu, 2019).

ML/DL (Machine Learning/Deep Learning) Open Set Recognition (OSR) problema, Gaussian Mixture Model (GMM) BI-LSTM-GMM.

e-ISSN: 2528-8091
Vol. 7, N° 3 - 2022

Con aprendizaje supervisado, el BI-LSTM se emplea para la discriminación de tráfico y ataques DDoS. Basado en un concepto similar al aprendizaje no supervisado, el GMM se adopta para construir el modelo de distribución de los datos de entrenamiento. Con GMM, nuevos ataques o se puede capturar nuevo tráfico legítimo si caen más allá de un rango específico de la construcción modelo de distribución. Los nuevos tráficos capturados están sujetos a la identificación y etiquetado del ingeniero de tráfico y luego se utiliza para actualizar el BI-LSTM y el GMM en la fase de aprendizaje incremental. Hasta cierto punto, el MMG puede considerarse como un clasificador de diferenciar muestras aprendidas e instancias novedosas y el BI-LSTM como clasificador para la discriminación de buenos y malos tráficos

El marco utiliza datos de tráfico históricos para que la formación de aprendizaje profundo genere modelos que

se pueden utilizar para detectar tráfico. También presentamos el módulo de mezcla gaussiana para hacer

que el modelo sea capaz de identificar ataques invisibles. Finalmente, ataques desconocidos o tráfico clasificados por el modelo de mezcla gaussiana serán identificados y etiquetados por expertos, y el modelo de aprendizaje profundo se actualizará a través del aprendizaje incremental (Shieh, 2021)

En cuanto a trabajos futuros en algunos casos analizados se combinan varias áreas de la inteligencia artificial para detección de patrones en la parte de análisis de datos, especialmente cuando DDoS de tipo LR(low rate).

CONCLUSIONES

- En este estudio se puede observar que la inteligencia artificial aporta el análisis de forma eficiente del conjunto de datos obtenido del entorno SDN, sin embargo, podemos notar que solo es una parte de muchas de las soluciones planteadas para mitigar los DDoS.

- Los algoritmos de inteligencia artificial utilizados tienen como entrada en la mayoría de los casos datos públicos esto contribuye a que los estudios realizados los atacantes conozcan que parámetros son considerados al momento de probar las soluciones para detección de patrones en los ataques DDoS.

e-ISSN: 2528-8091
Vol. 7, N° 3 - 2022

REFERENCIAS BIBLIOGRÁFICAS

Abdulqadder, I. H., Zou, D., Aziz, I. T., & Yuan, B. (2018). Validating User Flows to Protect Software Defined Network Environments. *Security and Communication Networks*, *2018*, 1-14. https://doi.org/10.1155/2018/1308678.

Akyildiz, I. F., Lee, A., Wang, P., Luo, M., & Chou, W. (2014). A roadmap for traffic engineering in SDN-OpenFlow networks. *Computer Networks*, *71*, 1-30. https://doi.org/10.1016/j.comnet.2014.06.002.

Aladaileh, M. A., Anbar, M., Hasbullah, I. H., Chong, Y.-W., & Sanjalawe, Y. K. (2020). Detection Techniques of Distributed Denial of Service Attacks on Software-Defined Networking Controller–A Review. *IEEE Access*, *8*, 143985-143995. https://doi.org/10.1109/ACCESS.2020.3013998.

Ashraf, J., & Latif, S. (2014). Handling intrusion and DDoS attacks in Software Defined Networks using machine learning techniques. *2014 National Software Engineering Conference*, 55-60. https://doi.org/10.1109/NSEC.2014.6998241.

Barcos, L. (2014). *Algoritmo basado en la optimización mediante colonias de hormigas para la resolución del problema del transporte de carga desde varios orígenes a varios destinos*. 10.

Cortada, P., & Sanromà, G. (2003). *IDS Based on Self-Organizing Maps*. 6.

Crs-cyber-risk-outlook-2019.pdf.

Cruz, I., Martinez, S. S., & Abed, A. R. (2007). *Redes neuronales recurrentes para el an8lisis de secuencias*. 11.

Deng, L. (2014). A tutorial survey of architectures, algorithms, and applications for deep learning. *APSIPA Transactions on Signal and Information Processing*, *3*, e2. https://doi.org/10.1017/atsip.2013.9.

Desjardins, G., Courville, A., Bengio, Y., Vincent, P., & Delalleau, O. (2010). Tempered Markov Chain Monte Carlo for training of Restricted Boltzmann Machines. *Proceedings of the Thirteenth International Conference on Artificial Intelligence and Statistics*, 145-152. http://proceedings.mlr.press/v9/desjardins10a.html

Dialnet-ANALISISDEPROXIMIDADDEMODELOSOCULTOSDEMARKOVPARALA-4829336.pdf.

Escobar, J. W., & Linfati, R. (2012). UN ALGORITMO METAHEURÍSTICO BASADO EN RECOCIDO SIMULADO CON ESPACIO DE BÚSQUEDA GRANULAR PARA EL PROBLEMA DE LOCALIZACIÓN Y RUTEO CON RESTRICCIONES DE CAPACIDAD. *Revista Ingenierías Universidad de Medellín*, *11*(21), 13.

García, S. Y. (s. f.). *Optimización mediante el algoritmo de colonia de abejas artificial*. 55.

Gestal, M. (2010). *Introducción a los algoritmos genéticos y la programación genética*. Universidade da Coruña, Servicio de Publicacións.

e-ISSN: 2528-8091
Vol. 7, N° 3 - 2022

Guo, M., Liu, Y., & Malec, J. (2004). A new Q-learning algorithm based on the metropolis criterion. *IEEE Transactions on Systems, Man, and Cybernetics. Part B, Cybernetics: A Publication of the IEEE Systems, Man, and Cybernetics Society*, *34*(5), 2140-2143. https://doi.org/10.1109/tsmcb.2004.832154

Herrera, F. (2015). Introducción a los Algoritmos Metaheurísticos. *Swarm Intelligence*, 129.

Hinton, G. E., Osindero, S., & Teh, Y.-W. (2006). A Fast Learning Algorithm for Deep Belief Nets. *Neural Computation*, *18*(7), 1527-1554. https://doi.org/10.1162/neco.2006.18.7.1527

Hurtado, S. M., & Gómez, G. P. (2008). *MODELO DE INFERENCIA DIFUSO PARA ESTUDIO DE CRÉDITO*. 15.

Javeed, D., Gao, T., & Khan, M. T. (2021). SDN-Enabled Hybrid DL-Driven Framework for the Detection of Emerging Cyber Threats in IoT. *Electronics*, *10*(8), 918. https://doi.org/10.3390/electronics10080918.

Jiang, Y., Zhang, X., Zhou, Q., & Cheng, Z. (2018). An Entropy-Based DDoS Defense Mechanism in Software Defined Networks. En Q. Chen, W. Meng, & L. Zhao (Eds.), *Communications and Networking* (Vol. 209, pp. 169-178). Springer International Publishing. https://doi.org/10.1007/978-3-319-66625-9_17

Kim, S., & Suk, J. (2016). Efficient peer-to-peer context awareness data forwarding scheme in emergency situations. *Peer-to-Peer Networking and Applications*, *3*(9), 477-486. https://doi.org/10.1007/s12083-015-0401-8.

Kreutz, D., Ramos, F. M. V., Esteves Verissimo, P., Esteve Rothenberg, C., Azodolmolky, S., & Uhlig, S. (2015). Software-Defined Networking: A Comprehensive Survey. *Proceedings of the IEEE*, *103*(1), 14-76. https://doi.org/10.1109/JPROC.2014.2371999

Kreutz, D., Ramos, F. M. V., & Verissimo, P. (2013). Towards secure and dependable software-defined networks. *Proceedings of the Second ACM SIGCOMM Workshop on Hot Topics in Software Defined Networking - HotSDN '13*, 55. https://doi.org/10.1145/2491185.2491199.

Latah, M., & Toker, L. (2019). Artificial Intelligence Enabled Software Defined Networking: A Comprehensive Overview. *IET Networks*, *8*(2), 79-99. https://doi.org/10.1049/iet-net.2018.5082

Lima, J., & Barán, B. (s. f.). *Inteligencia Artificial. Revista Iberoamericana*. *1*. https://www.redalyc.org/pdf/925/92503209.pdf

Liu, Z., Yin, X., & Hu, Y. (2020). CPSS LR-DDoS Detection and Defense in Edge Computing Utilizing DCNN Q-Learning. *IEEE Access*, *8*, 42120-42130. https://doi.org/10.1109/ACCESS.2020.2976706

López Ramos, D., Arco García, L., López Ramos, D., & Arco García, L. (2019). Aprendizaje profundo para la extracción de aspectos en opiniones textuales.

Revista Cubana de Ciencias Informáticas, *13*(2), 105-145.*Machine-Learning-7.pdf*.

Martínez, R. E. B., Ramírez, N. C., Mesa, H. G. A., Suárez, I. R., León, P. P., & Morales, S. L. B. (2009). *Árboles de decisión como herramienta en el diagnóstico médico*. 6.

Martínez-Lozano, J. E., & Atencio-Ortiz, P. S. (2019). Creation of a DDOS attack using HTTP-GET Flood with the Cyber Kill Chain methodology. *ITECKNE*, *16*(1), 41-47. https://doi.org/10.15332/iteckne.v16i1.2160.

Min, J., Yuejie, S., Qing, G., Zihe, G., & Suofei, X. (2020). *DDoS Attack Detection Method for Space-Based Network Based on SDN Architecture*. *18*(4), 8.

Mohammadi, M., Al-Fuqaha, A., Sorour, S., & Guizani, M. (2018). Deep Learning for IoT Big Data and Streaming Analytics: A Survey. *ArXiv:1712.04301 [Cs]*. http://arxiv.org/abs/1712.04301

Negnevitsky, M. (2005). *Artificial intelligence: A guide to intelligent systems* (2nd ed). Addison-Wesley.

Nunes, B. A. A., Mendonca, M., Nguyen, X.-N., Obraczka, K., & Turletti, T. (2014). A Survey of Software-Defined Networking: Past, Present, and Future of Programmable Networks. *IEEE Communications Surveys & Tutorials*, *16*(3), 1617-1634. https://doi.org/10.1109/SURV.2014.012214.00180

Ordoñez, H., Ordoñez, C., Cobos, C., & Torres-Jiménez, J. (2017). *Mejora de K-means usando arreglos de cubrimiento incrementales para la agrupación de procesos empresariales*. 15.

Rfc5810. (2007). Recuperado 24 de julio de 2021, de https://datatracker.ietf.org/doc/html/rfc5810.

Russell, S. J., & Norvig, P. (1995). *Artificial intelligence: A modern approach*. Prentice Hall.

Sánchez, F. (2016). *Diseño de un sistema de reconocimiento automático de matrículas de vehículos mediante una red neuronal convolucional*. 53.

Shieh, C.-S., Lin, W.-W., Nguyen, T.-T., Chen, C.-H., Horng, M.-F., & Miu, D. (2021). Detection of Unknown DDoS Attacks with Deep Learning and Gaussian Mixture Model. *Applied Sciences*, *11*(11), 5213. https://doi.org/10.3390/app11115213.

Tonkal, Ö., Polat, H., Başaran, E., Cömert, Z., & Kocaoğlu, R. (2021). Machine Learning Approach Equipped with Neighbourhood Component Analysis for DDoS Attack Detection in Software-Defined Networking. *Electronics*, *10*(11), 1227. https://doi.org/10.3390/electronics10111227.

Tosun, H. (2017). *Atomic Energy Models for Machine Learning: Atomic Restricted Boltzmann Machines*. 48.*V9N2A08 Lopez Boada.pdf*.

e-ISSN: 2528-8091
Vol. 7, N° 3 - 2022

Valencia, P. E. (2014.). *OPTIMIZACIÓN MEDIANTE ALGORITMOS GENÉTICOS*. 11.

Velásquez, J. D., Olaya, Y., & Franco, C. J. (2010). PREDICCIÓN DE SERIES TEMPORALES USANDO MÁQUINAS DE VECTORES DE SOPORTE. *Ingeniare. Revista chilena de ingeniería*, *18*(1), 64-75. https://doi.org/10.4067/S0718-33052010000100008.

Velásquez, R., & Candoti, K. (2015). METODOLOGÍA DE AJUSTE DE PARÁMETROS EN ALGORITMOS DE OPTIMIZACIÓN METAHEURÍSTICOS. . . *Pp.*, *6*(2), 20.