Contexto de aplicación.

Entre los ciberataques más comunes se encuentran la “denegación de servicios distribuida“ (DDoS o Distributed Denial of Service). Una DDoS ocurre cuando los atacantes utilizan múltiples dispositivos para agobiar un sistema, red o sitio web objetivo y disminuir sus recursos, lo cual, abruma la capacidad del objetivo para manejar solicitudes legítimas, volviéndola inaccesible para los usuarios legítimos. Los informes de Cisco-talos [1] y la división europea del CERT [2] vinculan el incremento de este tipo de ataques a las guerras entre Ucrania-Rusia, Israel-Hamás y el interés de terceros países en las regiones, donde se presenta el conflicto. Además de las referencias citadas, para ampliar este tema, se puede consultar [3]

Para contrarestar un DDoS, el primer paso es identificarlo y una opción es a través de un sistema de detección de intrusiones (IDS o Intrusion Detection System), el cual, se debe caracterizar por su velocidad para detectar irregularidades, precision y confiabilidad. La operación de un IDS consiste en una clasificación binaria del tráfico bajo análisis (normal o anómalo) o múlticlase (además, del tráfico normal, se identifican varios escenarios: R2R, U2R, DoS, DDoS, Probe, entre otros). Entre las técnicas de detcción de intrusión, tenemos:

- Detección anómala: Se verifica la actividad del sistema y se clasifica el tipo de tráfico (normal o anómalo). Generalmente, consiste de dos fases: 1. entrenamiento: Perfil de conducta normal es determinado. 2. Prueba: Tráfico actual se compara con perfil obtenido en la fase 1, para su identificación.

- Técnica de detección de uso indebido: Se detectan ataques a través de perfiles pre-configurados (patrones, firmas, otros); en este caso, se “conoce” la conducta anormal del sistema y si el tráfico no la cumple, se considera normal.

Para ampliar el tema de IDS, consultar [4], [5] y [6].

La evolución y crecimiento de Internet generó nuevos paradigmas para diseñar, implementar y gestionar redes de telecomunicaciones con características tales como, escalabilidad, seguridad, flexibilidad, desempeño, entre otras. Dentro de los paradigmas propuestos se encuentran las redes programables y uno de sus enfoques corresponde a las redes definidas por software (SDN o Software Defined Networks). La principal propiedad de la arquitectura SDN es la habilidad para separar las funciones de envió y control de la red, lo cual: 1. Facilita al admінitrador la gestión de dispositivos en la red, sin importar el vendedor. 2. Reduce la intervención humana.

La arquitectura lógica de SDN esta normalizada por la ONF y se describe commo:

- Plano de aplicación: se implementa a través de APIs, las cuale sexpandes las capacidades de los servicios SDN.

- Plano de control: Se implementa a través de controladores; los ontroladores son los responsables de informar las reglas de flujo en la red.

- Plano de datos: Se implementa a través de los dispositivos de interconexión y host, los cuales cumplen las reglas informadas por el controlador.

Para ampliar el tema de SDN, consultar [7], [8] y [9].

Nota: Información adicional para IDS consultar ; información adicional para SDN consultar [11], [12] y [13]; información adicional para estadísticas de ciberataques consultar [14], [15] y [16]

[1]
The most common cyber-attacks are web-based attacks, denial-of-service attacks, and malicious insider attacks.
We should identify the attack process firstly based on the IDS
Irregularity detection speed, accuracy, and reliability are the basic assessment factors for an IDS
This is attributed to the ability of CNNs to work on network traffic analysis as a pattern recognition problem.
The main property of an SDN architecture is that it has the ability to separate forwarding functions and network control.
This feature of SDN introduces several advantages. First, it facilitates network system management and reduces human intervention. In addition, it enables IT administrators to manage network devices without limitation to a particular vendor. Finally, it decreases operation cost compared with those of the conventional networks, since no programming language is required for the underneath infrastructure devices.
There are numerous difficulties for deploying IDS systems on the SDN standard. First, there is no public dataset that is available for anomaly detection systems. Most researchers use intrusion detection datasets. Unfortunately, current datasets just show specific types of attacks like DoS and DDoS, and the other attacks are ignored. In addition, these datasets belong to intrusions produced in a single component of the SDN. Attack vectors for different SDN layers are ignored.
The IDS operation depends on a classification task for the traffic in either a binary or multi-class classification scenario. In binary classification, we distinguish between normal and anomalous traffic classes. On the other hand, in multi-class classification, several classes such as Root-to-Local (R2L), User-to-Root (U2R), Denial-of-Service (DOS), and Probing (Probe) classes are considered.
Techniques of intrusion detection can be divided into anomaly detection and misuse detection techniques. In anomaly detection, the objective is to detect both network and computer intrusions by checking the system activity, and then classifying the type of traffic as being normal or anomalous. The classification here relies upon heuristics or rules. Most anomaly detection systems have two phases. The first is the training phase in which a profile of normal behavior is determined. The second is the testing phase in which current traffic is compared with the profile made in the training phase.
On the other hand, the main objective of misuse
detection is how to detect computer attacks. This is done by defining an abnormal system behavior at first, and then any deviation can be considered as a normal behavior. Misuse detection depends on patterns, signatures, or attempts. The advantage of using misuse detection is the simplicity of adding known attacks to the model. So, it is used more generally to refer to all kinds of computer misuse. The fundamental weakness of misuse detection is the inability to recognize unknown attacks. Hence, most intrusion detection systems depend on a combination of two techniques and are often deployed on the network, on a specific host, or even on an application within the host.
Anomaly detection has the ability to discover novel attacks in contrast to misuse detection. So, IDS with anomaly detection are applied on the SDN standard, but there is a problem. Threshold computing

methods or statistical measures are generally used to overcome network intrusions. These methods may not be efficient with complex attack patterns.
There is a need for learning of the long-term dependencies of temporal patterns in large-scale sequence data, in addition to hierarchical features. Object detection, detecting network intrusion, and visual object recognition are some applications that use deep learning algorithms. Supervised and unsupervised ways are used to train a deep learning algorithm. The CNN is illustrated as an example of deep learning algorithms that uses a supervised way for training. The CNN architecture is utilized in general in applications such as face recognition and 2D images.
The most widely-used activation function is the ReLU function.

To maintain a high level of security and network monitoring, it is required to allow machine learning and deep learning (ML/DL) approaches to be merged with SDN controllers. On the other hand, ML/DL approaches can be merged with SDN-based intrusion detection to introduce several advantages such as high Quality of Service (QoS), security enforcement, and virtual management. Other advantages introduced by SDN are enhancing the network security, eliminating hardware dependency and achieving flexibility to program network devices.

Objetivo de machine learning (queremos predecir X, dada tal información)

el objetivo es predecir si el tráfico recibido es anómalo y en caso afirmativo clasificar el tipo de ataque (de ser posible).

Dataset: tipo de datos, tamaño (número de datos y tamaño en disco), distribución de las clases

[17]

Métricas de desempeño (de machine learning y negocio)

Resultados previos

[1] This paper introduces an efficient IDS using Convolutional Neural Network (CNN). This IDS is applied on a new attack-specific SDN dataset called InSDN. The proposed IDS is compared in performance with different machine-learning-based systems such as Decision Tree Classifier (CART), Logistic Regression (LR), Support Vector Machine (SVM), Naïve Bayes (NB), Random Forest (RF) classifier, and AdaBoost (AB) classifier.

[2], [3], [4], [5], [6], [7]

Referencias

[1] https://blog.talosintelligence.com/cisco-talos-2023-year-in-review/

[2] https://www.ccn-cert.cni.es/es/informes/informes-ccn-cert-publicos/7188-ccn-cert-ia-35-23-ciberamenazas-y-tendencias-edicion-2023/file.html

[3] https://www.forbes.com/advisor/education/it-and-tech/cybersecurity-statistics/

[4] A. K. Saxena, S. Sinha and P. Shukla, "General study of intrusion detection system and survey of agent based intrusion detection system," 2017 International Conference on Computing, Communication and Automation (ICCCA), Greater Noida, India, 2017, pp. 471-421, doi: 10.1109/CCAA.2017.8229866.

[5] A. R. b. Gupta and J. Agrawal, "A Comprehensive Survey on Various Machine Learning Methods used for Intrusion Detection System," 2020 IEEE 9th International Conference on Communication Systems and Network Technologies (CSNT), Gwalior, India, 2020, pp. 282-289, doi: 10.1109/CSNT48778.2020.9115764.

[6] A. L. Giri and S. Annamalai, "Intrusion Detection System for Local Networks – A Review Study," 2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), Greater Noida, India, 2022, pp. 1388-1393, doi: 10.1109/ICACITE53722.2022.9823433.

[7] D. Kreutz, F. M. V. Ramos, P. E. Veríssimo, C. E. Rothenberg, S. Azodolmolky and S. Uhlig, "Software-Defined Networking: A Comprehensive Survey," in Proceedings of the IEEE, vol. 103, no. 1, pp. 14-76, Jan. 2015, doi: 10.1109/JPROC.2014.2371999.

[8] B. A. A. Nunes, M. Mendonca, X. -N. Nguyen, K. Obraczka and T. Turletti, "A Survey of Software-Defined Networking: Past, Present, and Future of Programmable Networks," in IEEE Communications Surveys & Tutorials, vol. 16, no. 3, pp. 1617-1634, Third Quarter 2014, doi: 10.1109/SURV.2014.012214.00180.

[9] J. Xie et al., "A Survey of Machine Learning Techniques Applied to Software Defined Networking (SDN): Research Issues and Challenges," in IEEE Communications Surveys & Tutorials, vol. 21, no. 1, pp. 393-430, Firstquarter 2019, doi: 10.1109/COMST.2018.2866942.

[1] H. A. Hassan, E. E. Hemdan, W. El-Shafai, M. Shokair and F. E. A. El-Samie, "An Efficient Intrusion Detection System for SDN using Convolutional Neural Network," 2021 International Conference on Electronic Engineering (ICEEM), Menouf, Egypt, 2021, pp. 1-5, doi: 10.1109/ICEEM52022.2021.9480383.

[2] A. H. Janabi, T. Kanakis and M. Johnson, "Convolutional Neural Network Based Algorithm for Early Warning Proactive System Security in Software Defined Networks," in IEEE Access, vol. 10, pp. 14301-14310, 2022, doi: 10.1109/ACCESS.2022.3148134.

[3] M. K, K. K, U. J, P. T, S. AR and S. D, "Classification of DDoS in Software-Defined IoT Networks using Hybrid Feature Selection Technique with DL," 2022 Third International Conference on Smart Technologies in Computing, Electrical and Electronics (ICSTCEE), Bengaluru, India, 2022, pp. 1-6, doi: 10.1109/ICSTCEE56972.2022.10099827.

[4] Y. Wang, X. Yi, Z. Bao and B. Yu, "An Effective Anomaly Detection Model Combined Feature Selection with Improved CNN in SDN," 2023 3rd Asia-Pacific Conference on Communications Technology and Computer Science (ACCTCS), Shenyang, China, 2023, pp. 281-287, doi:

10.1109/ACCTCS58815.2023.00048.

[5] H. A. Hassan, E. El-Din Hemdan, M. Shokair, F. E. A. El-Samie and W. El-Shafai, "An Efficient Attack Detection Framework in Software-Defined Networking using Intelligent Techniques," 2023 3rd International Conference on Electronic Engineering (ICEEM), Menouf, Egypt, 2023, pp. 1-6, doi: 10.1109/ICEEM58740.2023.10319575.

[6] R. B. Said and I. Askerzade, "Attention-Based CNN-BiLSTM Deep Learning Approach for Network Intrusion Detection System in Software Defined Networks," 2023 5th International Conference on Problems of Cybernetics and Informatics (PCI), Baku, Azerbaijan, 2023, pp. 1-5, doi: 10.1109/PCI60110.2023.10325985.

[7] R. Ben Said, Z. Sabir and I. Askerzade, "CNN-BiLSTM: A Hybrid Deep Learning Approach for Network Intrusion Detection System in Software-Defined Networking With Hybrid Feature Selection," in IEEE Access, vol. 11, pp. 138732-138747, 2023, doi: 10.1109/ACCESS.2023.3340142

[17] M. S. Elsayed, N. -A. Le-Khac and A. D. Jurcut, "InSDN: A Novel SDN Intrusion Dataset," in IEEE Access, vol. 8, pp. 165263-165284, 2020, doi: 10.1109/ACCESS.2020.3022633