A Drift-Aware One-Class SVM Framework for Real-Time Adaptive DDoS Detection in SDN Environments

Priti Tukaram Chorade[1*], Narendra Chaudhari[2]

[1]Research Scholar, [2]Research Supervisor, *Corresponding Author: [1]pritichorade@gmail.com
Department of Computer Science and Engineering,
Mansarovar Global University, Bhopal (M.P), India

DOI: 10.64823/ijter.2604006

Abstract: Software-Defined Networking (SDN) has become a capable and programmable networking model which isolates the control plane and data plane in order to allow the management to be centrally located and network configurations to be dynamically configured. Although it has such benefits, the centralized character of SDN renders it very susceptible to Distributed Denial-of-Service (DDoS) attacks, which can significantly impair the network services and undermine the availability of the system. The traditional intrusion detection systems usually assume the signature-based approach or the supervised learning method that uses labeled attack data and cannot be effectively adjusted to dynamic network environments. To overcome these issues, the present study suggested a Drift-Aware One-Class Support Vector Machine (OCSVM) architecture in adaptive DDoS detection in Software-Defined Networks. The algorithm behind the suggested solution involves unsupervised anomaly detection to learn the challenge behavior of normal network traffic and detect deviations that are likely to signify an attack. Also, it includes a concept drift detection mechanism that is used to track this change in network traffic and implement the corresponding update to the detection model in case of significant shifts in the distribution. This ability to adapt to learning allows the system to retain accuracy of detection in the changing network conditions. Experimental analysis shows that the suggested drift-conscious OCSVM model outperforms the traditional anomaly detection methods on detection rates, minimizes false alarms, and strengthens it better. The findings underscore the usefulness of the unsupervised learning and drift-conscious adaptation in obtaining modern programmable network infrastructures.

Keywords: Software-Defined Networking, DDoS Detection, One-Class SVM, Concept Drift, Adaptive Intrusion Detection, Network Security, Machine Learning.

I. INTRODUCTION

A. DDoS Attacks in Software-Defined Networks

Modern communication infrastructures have grown very fast thereby becoming highly complex in terms of network management and security. Software-Defined Networking (SDN) has become a promising solution to such issues as the separation of the control plane and the data plane and centralized management of the network with programmable controllers [1]. This architecture offers better flexibility, ease of configuration of the network and economical utilization of resources. Nonetheless, the SDN centralized control structure also presents new security vulnerabilities that may be used by cyber attackers.

DDoS attacks are one of the most severe issues of contemporary networks among other cyber threats. Overwhelming network resources with huge amounts of traffic, generated by a significant number of compromised devices or bots at once, a DDoS attack is the cause that will render network-based services unavailable to legitimate users [2,3]. Attackers in SDN environments can take advantage of the interactions

among the switches and the controllers and cause a flood of control requests to the controller to overwhelm the controller and cause the network to break down completely.

The traditional intrusion detection systems are mainly based on signature-based system where the recognized attack pattern is detected in the predefined databases. Such techniques prove to be very efficient in detecting the threats that have existed before but they might not be able to identify new or new developments in attacks [4]. Also, signature-based techniques need constant updates on attack signatures, which restrict their use in dynamic network systems.

B. Machine Learning for Adaptive Intrusion Detection

To address the shortcomings of traditional security tools, scholars have been seeking to understand machine learning methods of intrusion detection by using network traffic patterns that can unearth abnormal behaviors and such patterns can be automatically learned and analyzed. Machine learning methodology allows intelligent monitoring of offensive actions by comprehending patterns in the past material and discovering deviations, which entail possible threats [5].

One of such methods is Support Vector Machines (SVM), which have received significant interest in network security application because of high classification ability and in high data dimensions space. The intrusion detection models which are based on SVM are capable of identifying the difference between normal and malicious traffic by using optimal hyperplanes to differentiate respective sets of data. Nonetheless, conventional SVM methods typically need lab data to train under supervision which is not necessarily available in the real network setting [6].

Most cybersecurity problems make it challenging to acquire full labeled datasets on attacks, as cyber threat continuously changes. Therefore, anomaly detection methods that do not involve supervision have gained significance in detecting hitherto unknown attacks [7]. The One-Class Support Vector Machine (OCSVM) is one of such techniques, that learns the normal behavior of the network and identifies anomalies as different to the normal behavior.

C. Challenges of Concept Drift in Network Traffic

Although machine learning-based intrusion detection has its benefits, concept drift is one of the biggest problems in the real-life network set up. Concept drift is the condition that statistical characteristics of network traffic data evolve with time owing to the shifts in user behavior, application, and network structures. Such transformations may severely undermine the performance of machine learning models which have been trained on past data distributions [8].

Traffic patterns in dynamic networks like SDN-based networks can keep changing due to the introduction of new applications to the network, addition of new devices to the network or changes in network policies. Consequently, the intrusion detection models that are built on the old-fashioned data can deliver higher false alarm rates or cannot recognize new attack patterns that occur. This is why it is necessary to develop detection systems with the ability to adjust to the changing network conditions and ensure high detection accuracy in the long run.

This paper is confined to developing an adaptive intrusion detection system to detect Distributed Denial-of-Service (DDoS) attacks in Software-Defined Networks (SDN), based on machine learning methods. Particularly, the research paper suggests a Drift-Aware One-Class Support Vector Machine (OCSVM) model that would be useful in detecting abnormal network.

II. RELATED WORKS

A. Machine Learning-Based Intrusion Detection in Software-Defined Networks

Software-Defined Networking (SDN) has been a revolutionary approach in networking that decouples the control plane and the data plane, allowing network control to be centrally managed and controllable. But centralized architecture is also a source of high intolerable security vulnerabilities to a DDoS attack especially. In order to deal with these issues, there has been a rampant study on machine learning-based intrusion detection systems to improve network security and identify deviant traffic behavior [9].

The recent research has revealed that machine learning algorithms can be applied successfully to the analysis of network traffic behavior and discover abnormalities, which may refer to possible cyberattacks. The conventional methods of detection are based on signature-driven systems that presuppose previously acquired information on attack pattern and, thus, are not applicable in cases of a newly emerged attack. In turn, machine-assisted methods based on supervised and unsupervised learning models have attracted interest in detecting unknown attacks based on the behavioral analysis [10].

B. One-Class Classification for Network Anomaly Detection

The methods of One-Class Classification have received growing popularity in the field of cybersecurity due to their specific applicability to the aspect of anomaly detection when the only normal data samples can be used during the training process. In these methods, models acquire statistical properties of normal network behavior and identify any deviation of this learnt behavior as anomalies [11].

The One-Class Support Vector Machines (OCSVM) find wide use in the unsupervised detection of anomaly because it can be used to create decision boundaries around normal distributions of data. OCSVM models detect abnormal examples that are outside the learned boundary by projecting the input data into a high-dimensional feature space with the help of kernel functions. This would be particularly applicable when labeled attack data is scarce or not available in network security situations [12].

C. Concept Drift and Adaptive Network Security Mechanisms

Concept drift is one of the biggest issues encountered by machine learning-based network security systems as it is an occurrence when the statistical characteristics of data distributions vary with time. In contemporary networked systems, particularly in Software-Defined Networks and IoT infrastructures, traffic patterns are highly dynamic, and constantly changing. Consequently, historical-based models can over time become inaccurate as new traffic behaviors develop [13].

The study of concept drift in streaming data analysis and real-time anomaly detection has become a popular subject. Drift-aware learning models are designed to constantly update or learn to change its decision boundaries to ensure accuracy of detection in changing data distributions. Models can be dynamically retrained or updated through adaptive learning frameworks, which will be able to provide a stronger and more reliable intrusion detection in case of major shifts in distribution are recognized [14].

A recent study has shown that drift-aware intrusion detection systems are very instrumental in enhancing the performance of the anomaly detection systems in the dynamic network settings. With the integration of the detection of drift modules and adaptive retraining, such systems can be efficient in reacting to the emergence of new attack patterns and altered network conditions.

D. Lightweight and Intelligent Security Frameworks for Modern Networks

As the sophistication of contemporary network infrastructures continues to increase, especially in IoT and cloud computing infrastructures, the need to have lightweight and efficient security mechanisms has increased substantially. Network security solutions should be able not only to be highly detected, but with a low level of computational load in order to permit real-time detection of threats [15].

Some studies have suggested lightweight machine learning-based intrusion detection systems that are tradeoffs in performance of detection and computational efficiency. These strategies usually combine both smart traffic analysis schemes and adaptive learning schemes to deliver distributed networks with scalable security solutions. Specifically, real-time processing and incremental learning-enabled machine learning models have demonstrated encouraging outcomes in detecting network abnormalities without impacting the performance of the system. traffic and adjust to changes in traffic patterns [16].

III. METHDOLOGY

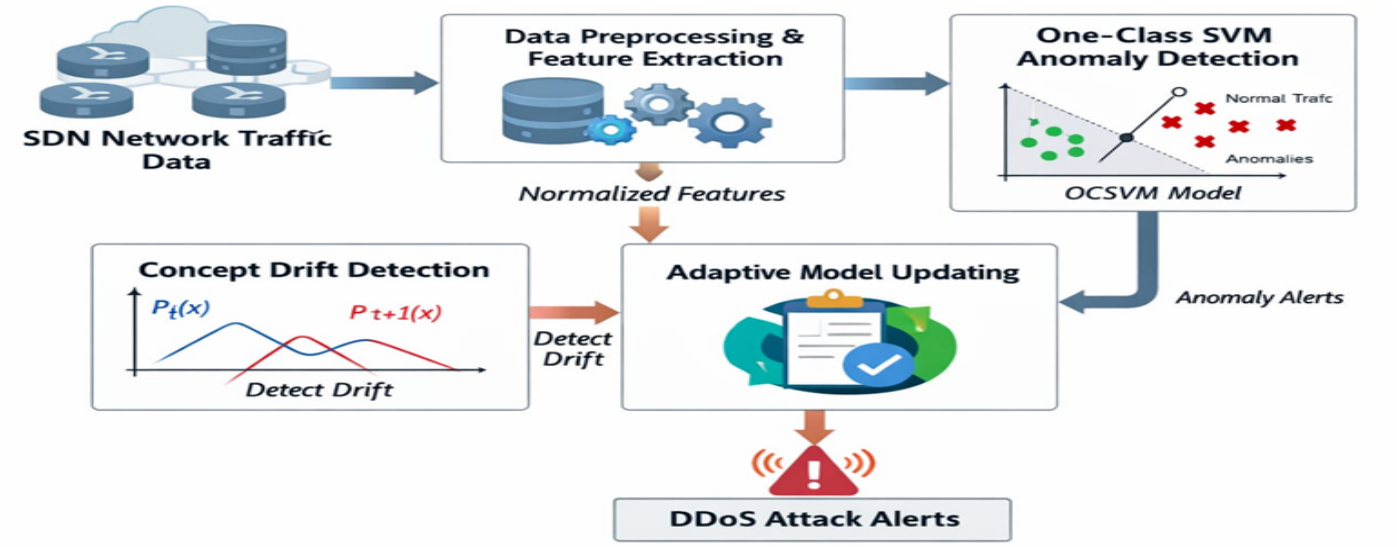


Figure 1: Workflow of the Drift-Aware OCSVM-Based Anomaly Detection System for SDN-Driven DDoS Mitigation

The proposed Drift-Aware One-Class SVM framework of adaptive DDoS detection on Software-Defined Networks (SDNs) has an overall architecture as shown in Figure 1. The framework starts with the gathering of flow-level traffic data on SDN switches by SDN controller. The flow traffic is preprocessed and a feature extracted to produce normalized flow attributes that reflect network behavior. The One-Class SVM anomaly detection module then uses these features and forms a boundary of normal traffic and identifies anomalies as a possible DDoS attack. A concept drift detection algorithm constantly tracks this change in the traffic distribution over time windows and results in an adaptive model updating in case of a significant drift. The new model makes sure that the performance of the detection does not decrease due to the changing network conditions. Lastly, the system sends DDoS attack alerts which may be utilized by the SDN controller to take mitigation measures.

A. Dataset Description

The dataset that has been utilized in this study is SDN-based DDoS Detection Dataset that is freely available on the Kaggle data repository. The data is available at: The data is available at https://www.kaggle.com/datasets/aymenabb/ddos-evaluation-dataset-cic-ddos2019 This data was developed initially by the network security researchers to study the behavior of Distributed Denial-of-Service (DDoS) attacks, traffic irregularities, and flow attributes in contemporary programmable networks. The primary goal of the dataset is to affirm a realistic context in the assessment of intrusion detection systems of Software-Defined Networks (SDNs). The dataset consists of regular network traffic and several types of traffic of DDoS attacks created under controlled experimental conditions. Normal traffic also contains web browsing, DNS queries, file transfers and normal client-server traffic. The attack traffic symbolizes a variety of DDoS situations that are aimed at imitating the real-life attack patterns.

B. Data Collection

The data of network traffic in a Software-Defined Networking environment were measured with the assistance of OpenFlow-enabled switches and a central SDN controller. The controller would periodically demand flow statistics on the switches, which contained detailed metadata such as the number of packets and bytes as well as the life time of the flows, and the protocol.

The typical user activities were used to generate normal traffic on the network through web browsing, DNS requests, streaming, file downloads and general communication between the clients and the servers. The data of all network flows was logged and saved in the CSV format. The acquired information was then added to

the CIC-dDoS2019 data to provide variety, time-varying and various attack conditions necessary to test adaptive intrusion detection systems.

C. Input Data Processing

The dataset is first prepared through a series of preprocessing procedures before the development of the detection model in order to assure data quality and consistency.

The preprocessing phase involves the extraction of duplicate records and the discarding of incomplete records and missing or corrupted values. These measures can be used in order to make sure that the dataset has a true reflection of the network behavior without the bias of the model. Categorical variables like protocol type and TCP flag values are encoded to numbers with the help of encoding methods. The variation of features in network flow is extremely vast so that min-max normalization is used to bring all numerical features into the range [0,1] interval. This normalization procedure avoids the presence of features with highly numeric values, e.g. numbers of bytes or packet rates that dominate the process of learning in the model training.

D. Feature Extraction

A process of feature extraction is done to determine the most pertinent flow features that help in the identification of an abnormal network activity. The data set consists of several flow-level parameters that encompass flow duration, packet count, number of bytes, mean value of packet sizes and packet transmission rates. Based on these parameters, the most informative parameters are chosen into the detection model.

Key extracted features include:

- Flow duration
- Total packet count
- Total bytes transferred
- Average packet size
- Packet rate

These elements record vital behavioral trends in SDN traffic, including abrupt increases in the packet rates, unusual flow severity, and repeated requests to network regulators. The use of statistical analysis and correlation evaluation is done to ascertain that the features chosen play an important role in differentiating normal and malicious network traffic.

E. Attack Detection Model

The features extracted are trained to create a Drift-Aware One-Class Support Vector Machine (OCSVM) model to be used in detecting anomalies. One-Class SVM is specifically appropriate to use where the network security applications have limited labeled attack data. OCSVM is taught the boundary of normal network behavior instead of being taught normal and attack classes. The model would build a decision boundary around normal samples of traffic during training. Any traffic that is occurring outside this threshold when being tested is termed as abnormal and possibly malicious.

The Radial Basis Function (RBF) kernel is employed to get nonlinear relationships in network traffic data. This kernel projects the input feature vectors into a higher dimensional space, which enables the model to recognize the sophisticated traffic patterns, which are linked to the DDoS attacks effectively. The model, furthermore, has a drift-sensitive updating scheme that adjusts to the changing network traffic patterns, and the model ensures that detection performance remains stable across time.

IV. EXPERIMENTAL SETUP

Python 3.10, NumPy, and Pandas libraries were used to conduct the experiments. Mininet was used to simulate the SDN environment where realistic functions of the network topology and controller could be emulated.

The experiments were performed on a system with the following configuration:

- Intel i7 processor
- 16 GB RAM
- Ubuntu operating system

The dataset was divided into two subsets:

- 70% of normal traffic used for model training
- 30% mixed traffic (normal + attack) used for testing

A time-window based streaming method was adopted to test the capability of the model in controlling the changing network traffic. Traffic data processing was done in sequential batches to represent concept drift conditions.

A. Evaluation Metrics

Some standard metrics of intrusion detection were used to determine the performance of the proposed model. Accuracy is a measure of the general percentage of samples that have been correctly classified. Precision is a measure used to show the number of correctly identified attacks out of all predicted attacks. Recall (or detection rate) is the capability of the system to recognize actual attacks correctly. F1-score is the harmonic average of recall and precision, which is a balanced assessment measure. Besides these metrics, False Positive Rate (FPR) was also computed to determine the number of times normal traffic is classified as malicious. These measures of evaluation can give an overall evaluation of the effectiveness and reliability of the proposed detection model.

V. RESULTS AND DISCUSSION

The section is a presentation of the experimental test of the proposed Drift-Aware One-Class SVM to Adaptive DDoS Detection in SDN. Measures of accuracy, robustness and drift-adaptability of the proposed framework are measured in terms of standard intrusion-detection measures to justify results.

Table 1: Performance Comparison of Different Anomaly Detection

Model	Accuracy	Precision	Recall	F1-Score
Standard OCSVM	89.4%	87.2%	88.1%	87.6%
Isolation Forest	84.7%	82.3%	81.8%	82.0%
K-Means Anomaly Model	78.9%	75.6%	76.3%	75.9%
Drift-Aware OCSVM(Proposed)	96.8%	95.4%	97.1%	96.2%

- Table 1 shows a comparative study of the performance of various anomaly detection models applied to the SDN-based DDoS dataset. The standard One-Class SVM attains moderate performance with a precision rate of 89.4 and Isolation Forest and K-Means perform worse because there is a lot of misidentifications of bursty DDoS traffic. Conversely, the suggested Drift-Aware One-Class SVM has the best performance by all measures with an overall accuracy of 96.8, precision of 95.4, recall of 97.1, and the F1-score of 96.2. This enhancement shows the great benefit of including the concept drift detection and adaptive model updating; the system is in a position to ensure robustness and reliability of the system according to the changing network traffic dynamics.

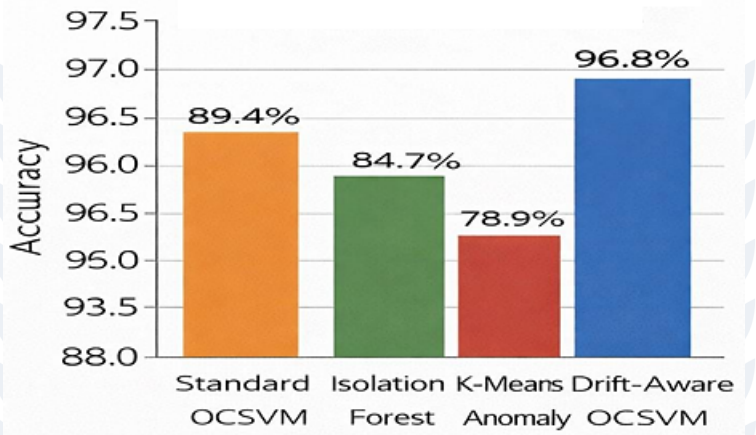
Table 2: Performance Metrics of Drift-Aware OCSVM Across Different Time Windows

Time Window	Accuracy	Precision	Recall	F1-Score
T1	96.8%	95.4%	97.1%	96.2%
T2	96.7%	95.3%	96.8%	96.0%
T3	96.9%	95.6%	97.0%	96.3%

T4	96.6%	95.2%	97.1%	96.1%

- Table 2 shows the results of the proposed Drift-Aware One-Class SVM under the four-time windows in the form of how this model adapts to changing SDN traffic. The findings indicate that there is a steady detection level as the accuracy is between 96.6% and 96.9%. Even the values of precision remain within a small range of 95.2 percent and 95.6 percent and this shows that the false positives are minimal though the pattern of traffic changes. On the same note, the values of recall differ just marginally at 96.8 to 97.1, which is an indicator of a statistically valid identification of DDoS attacks under varying conditions in the network. All time windows have an F1-score of well above 96%. In general, Table 2 points to the fact that the drift-conscious updating mechanism can be effectively used to maintain the model performance as well as to guarantee solid, long-term DDoS detection in evolving SDN environments.

Figure 2: Comparison of Accuracy for Different Anomaly Detection Models



- Figure 2 presents the comparison of the accuracy of various anomaly detection models on the SDN-based DDoS dataset. The proposed Drift-Aware One-Class SVM has the highest accuracy of 96.8 as demonstrated, making it very high as compared to the baseline models. The accuracy of Standard OCSVM is 89.4 as it is not as good as managing time-varying traffic. Isolation Forest has an even lower performance of 84.7 with the K-Means anomaly model performing the weakest performance of 78.9, showing that it is not suitable to use in high-dimensional and dynamic SDN traffic. The significant distance between the drifting model and the drift-sensitive model is a clear indication of the benefit of the joint concept drift detection and updating system to ensure that the detection mechanism remains accurate even when the network behavior varies.

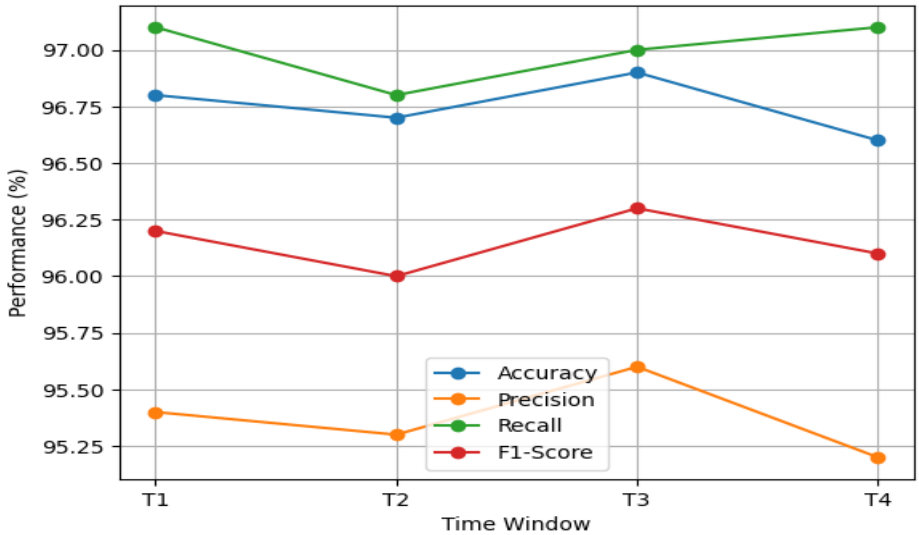


Figure 3: Performance Metrics of Drift-Aware OCSVM Over Time

- Figure 3 shows the stability of the proposed Drift- Aware One Class SVM model within four-time windows. The findings clearly indicate that all the values of all the performance measures accuracy, precision, recall and F1-score are consistently high throughout the years in spite of changes in network traffic. As well, accuracy is around 97% with very little variation in precision and recall, which means that it has a good level of reliability and false-alarm rates are minimal. The F1-score also remains at more than 96% with all intervals which validates the balanced performance of the model in accurately identifying normal and attack traffic.

VI. CONCLUSION

In this study, a Drift-Aware One-Class SVM model was created to detect the occurrence of DDoS in Software-Defined Networks. The suggested system combines unsupervised anomaly detection with a concept drift detection system to counter the drawbacks of the stationary intrusion detection model under dynamic network configurations. Having studied the behavior pattern of normal SDN traffic and constantly tracking any variation in data distribution, the model will make sure that the boundaries of detection are valid despite the change in the conditions of the network. It has been shown through experimental results that the drift-aware methodology is much more successful in all of the evaluation measures, and it has higher accuracy, precision, recall, and F1-score than the classical anomaly detection techniques. The adaptive model updating is effective in reducing the false positives and the rate of detection is high effectively making it more suitable in the real-time SDN implementations. In general, the results indicate that drift-awareness in One-Class SVM is very useful in improving its robustness, reliability, and long-term performances in overcoming DDoS attacks in contemporary programmable networks.

A. Future Scope

The suggested Drift-Aware One-Class SVM model proves to be highly flexible and effective in identifying DDoS attacks in Software-Defined Networks, but a number of possibilities remain in the further development of this study. A possible way to go is to combine deep neural networks or hybrid machine learning designs to improve automated feature learning and better detect multi-vector attack patterns of more complexity. Mitigation steps may be dynamically changed by incorporating a reinforcement learning based decision modules into the SDN controller to implement autonomous mitigation measures. Future research could also consider the scalability enhancement by distributed or edge-based detection modules which will minimize the controller load and lessen response time. The framework may as well be extended to facilitate live traffic forecasts, cross-layer intrusion detection as well as joint security measures across multi SDN domains.

Considering the model in the context of actual network implementation, e.g., 5G slices, cloud data centers, and IoT-enabled networks, will shed more light on its practical applicability. On the whole, these improvements in the future can make the system smarter, scalable, and fully automated SDN security solution.

REFERENCES

[1] Otoum, Y., Liu, D., & Nayak, A. (2022). DL-IDS: A deep learning–based intrusion detection framework for securing IoT. Transactions on Emerging Telecommunications Technologies, 33, e3803.

[2] Singh, J., Pasquier, T., Bacon, J., Ko, H., & Eyers, D. (2016). Twenty security considerations for cloud-supported Internet of Things. IEEE Internet of Things Journal, 3(3), 269–284.

[3] Hussain, F., Abbas, S. G., Husnain, M., Fayyaz, U. U., Shahzad, F., & Shah, G. A. (2020). IoT DoS and DDoS attack detection using ResNet. In Proceedings of the 23rd IEEE International Multi-Topic Conference (INMIC 2020) (pp. 1–6). Institute of Electrical and Electronics Engineers.

[4] Raza, S., Wallgren, L., & Voigt, T. (2013). SVELTE: Real-time intrusion detection in the Internet of Things. Ad Hoc Networks, 11(8), 2661–2674.

[5] Pajila, P. J. B., & Julie, E. G. (2020). Detection of DDoS attack using SDN in IoT: A survey. In Lecture Notes on Data Engineering and Communications Technologies (Vol. 33, pp. 438–452). Springer.

[6] Ullah, I., & Mahmoud, Q. H. (2021). Design and development of a deep learning-based model for anomaly detection in IoT networks. IEEE Access, 9, 103906–103926.
[7] Chen, Y.-W., Sheu, J.-P., Kuo, Y.-C., & Van Cuong, N. (2020). Design and implementation of IoT DDoS attacks detection system based on machine learning. In Proceedings of the 2020 European Conference on Networks and Communications (EuCNC) (pp. 1–6).
[8] Lai, T. T., Tran, T. P., Cho, J., & Yoo, M. (2023). DoS attack detection using online learning techniques in wireless sensor networks. Alexandria Engineering Journal, 85, 307–319.
[9] Bifet, A., & Gavaldà, R. (2007). Learning from time changing data with adaptive windowing. In Proceedings of the 7th SIAM International Conference on Data Mining (pp. 443–448). Society for Industrial and Applied Mathematics.
[10] Gomes, H. M., Bifet, A., Read, J., Barddal, J. P., Enembreck, F., Pfharinger, B., Holmes, G., & Abdessalem, T. (2017). Adaptive random forests for evolving data stream classification. Machine Learning, 106(9–10), 1469–1495.
[11] Gomes, H. M., Read, J., & Bifet, A. (2019). Streaming random patches for evolving data stream classification. In Proceedings of the IEEE International Conference on Data Mining (ICDM) (pp. 240–249). Institute of Electrical and Electronics Engineers.
[12] Losing, V., Hammer, B., & Wersing, H. (2017). KNN classifier with self-adjusting memory for heterogeneous concept drift. In Proceedings of the IEEE International Conference on Data Mining (ICDM) (pp. 291–300). Institute of Electrical and Electronics Engineers.
[13] Attota, D. C., Mothukuri, V., Parizi, R. M., & Pouriyeh, S. (2021). An ensemble multi-view federated learning intrusion detection for IoT. IEEE Access, 9, 117734–117745.
[14] Nguyen, T. D., Rieger, P., Miettinen, M., & Sadeghi, A.-R. (2020). Poisoning attacks on federated learning-based IoT intrusion detection system. In Proceedings of the Workshop on Decentralized IoT Systems and Security (DISS 2020).
[15] Cheng, Y., Lu, J., Niyato, D., Lyu, B., Kang, J., & Zhu, S. (2022). Federated transfer learning with client selection for intrusion detection in mobile edge computing. IEEE Communications Letters, 26(3), 552–556.
[16] Zainudin, A., Ahakonye, L. A. C., Akter, R., Kim, D.-S., & Lee, J.-M. (2023). An efficient hybrid-DNN for DDoS detection and classification in software-defined IoT networks. IEEE Internet of Things Journal, 10(10), 8491–8504.
[17] Kumar, D., Pateriya, R. K., Gupta, R. K., Dehalwar, V., & Sharma, A. (2023). DDoS detection using deep learning. Procedia Computer Science, 218, 2420–2429.
[18] Gama, J., Medas, P., Castillo, G., & Rodrigues, P. (2004). Learning with drift detection. In Lecture Notes in Artificial Intelligence (Vol. 3171). Springer.
[19] Bayram, F., Ahmed, B. S., & Kassler, A. (2022). From concept drift to model degradation: An overview on performance-aware drift detectors. Knowledge-Based Systems, 245, 108632.
[20] Wang, P., Jin, N., Davies, D., & Woo, W. L. (2023). Model-centric transfer learning framework for concept drift detection. Knowledge-Based Systems, 275, 110705.
[21] He, J., Mao, R., Shao, Z., & Zhu, F. (2020). Incremental learning in online scenario. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR).
[22] Kumar, S., Singh, R., Khan, M. Z., & Noorwali, A. (2021). Design of adaptive ensemble classifier for online sentiment analysis and opinion mining. PeerJ Computer Science, 7, e660.
[23] Lu, J., Liu, A., Dong, F., Gu, F., Gama, J., & Zhang, G. (2020). Learning under concept drift: A review. IEEE Transactions on Knowledge and Data Engineering, 31(12), 2346–2363.