

Towards Securing the Software-Defined Networks (SDN) using Machine Learning Techniques

Dr. Anca D. Jurcut

School of Computer Science, University College Dublin, Ireland

Email: anca.jurcut@ucd.ie

Preview

- Background and Motivation
- SDN Security Challenges
- Anomaly via Intrusion
- Anomaly Based Solutions in SDNs
- Visual Abstract
- Contributions
- Defense-in-Depth
- Looking Ahead
- Publications

Background and Motivation

How to easily configure huge networks?

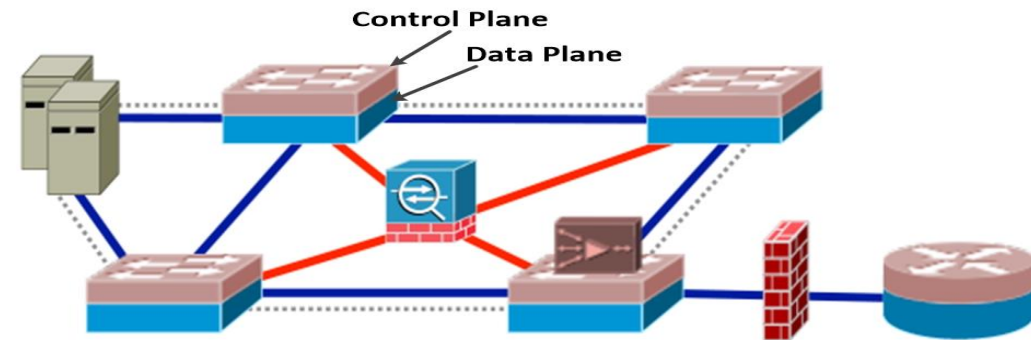


Figure 1: IP-Traditional Networking

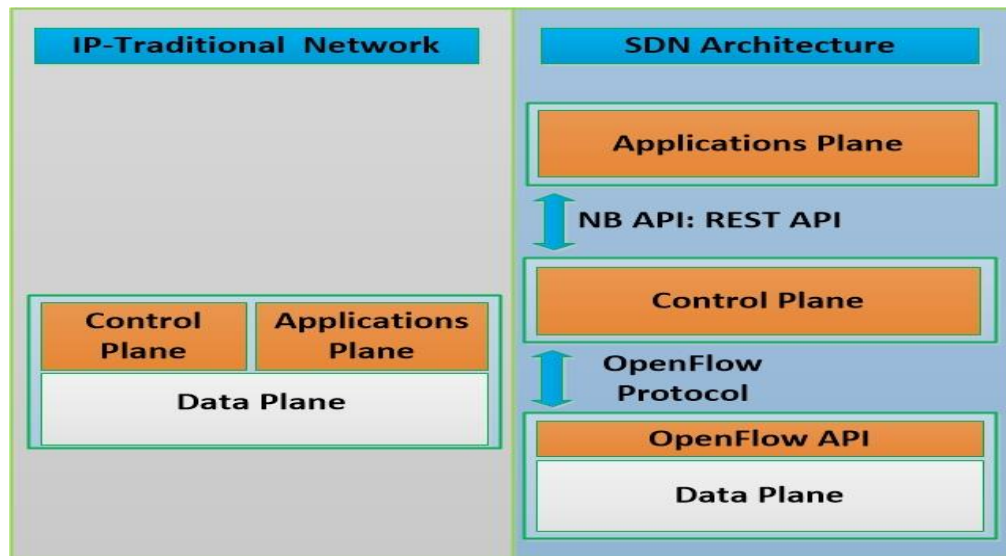


Figure 2: Traditional vs SDN architecture

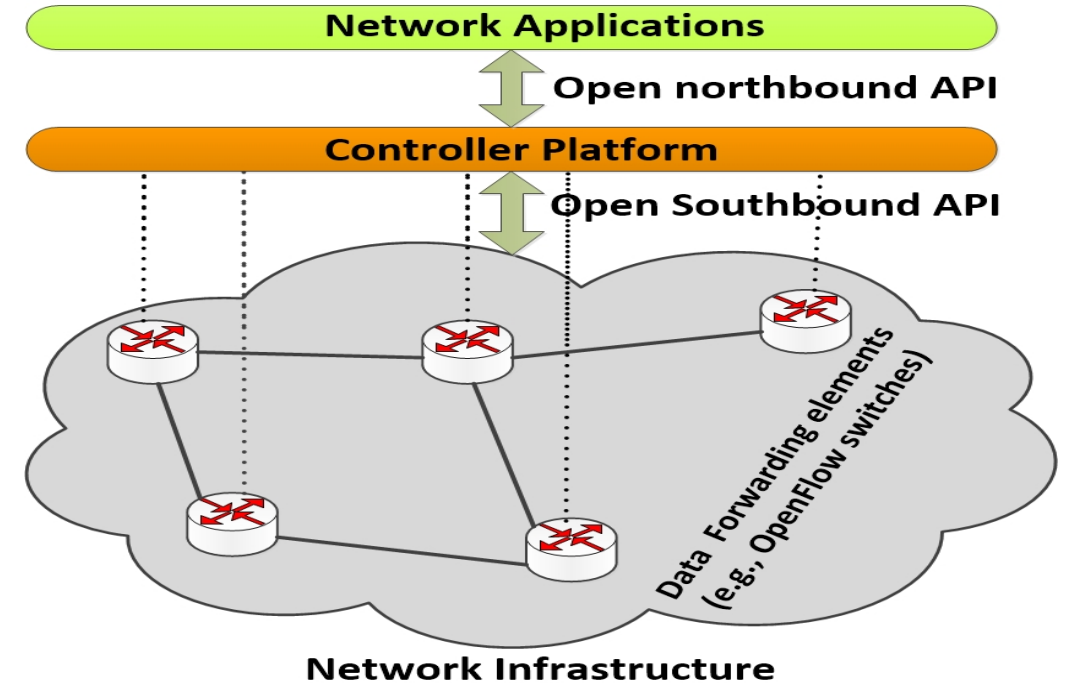


Figure 3: Software-Defined Networking

- ❖ The SDN architecture decouples the network control and forwarding functions.
- ❖ the data plane devices (network switches) become simple forwarding devices.

Background and Motivation

- ❖ The enormous benefits of SDN are making its market continuously growing.
- ❖ As a result, it achieved \$8 billion at the end of 2020 and this value is expected to reach \$43.3 billion by 2027.

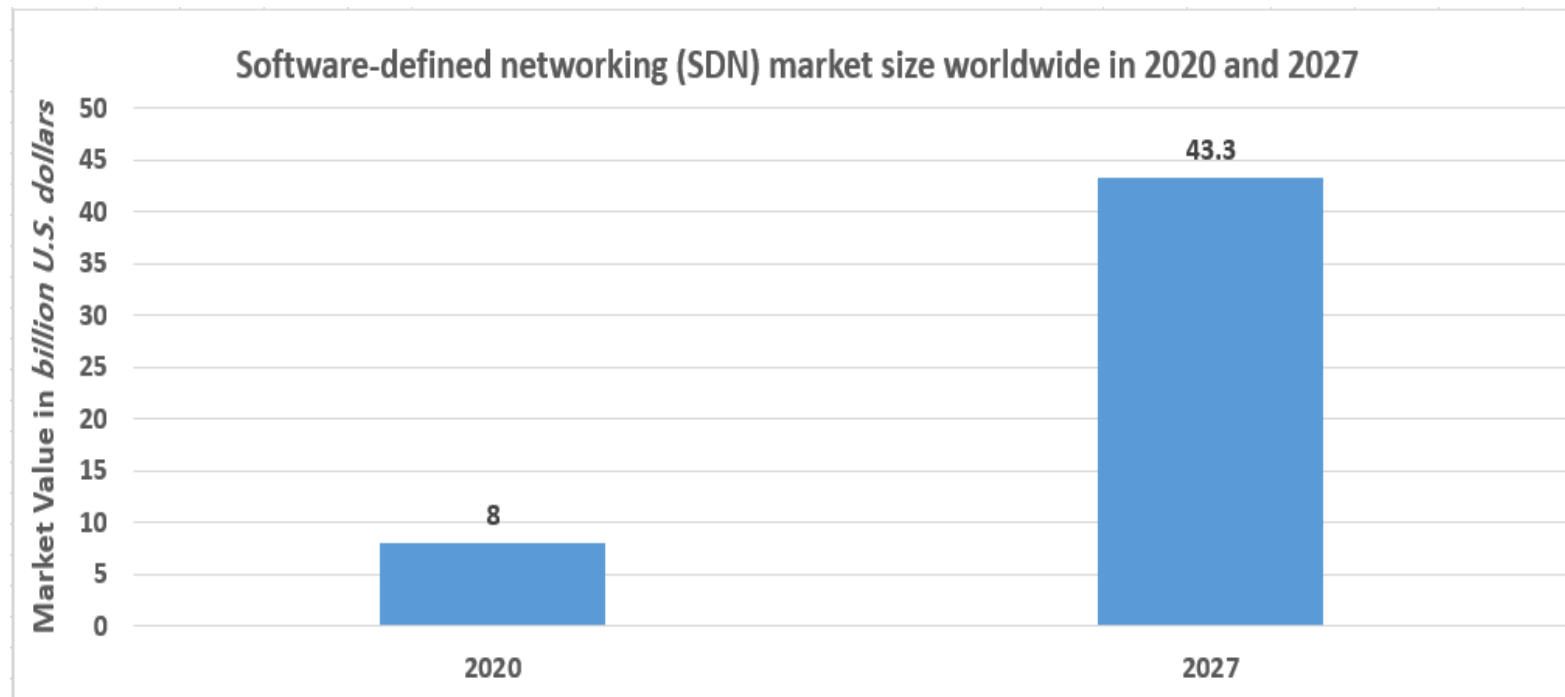


Figure 4: SDN market size prediction.

Background and Motivation

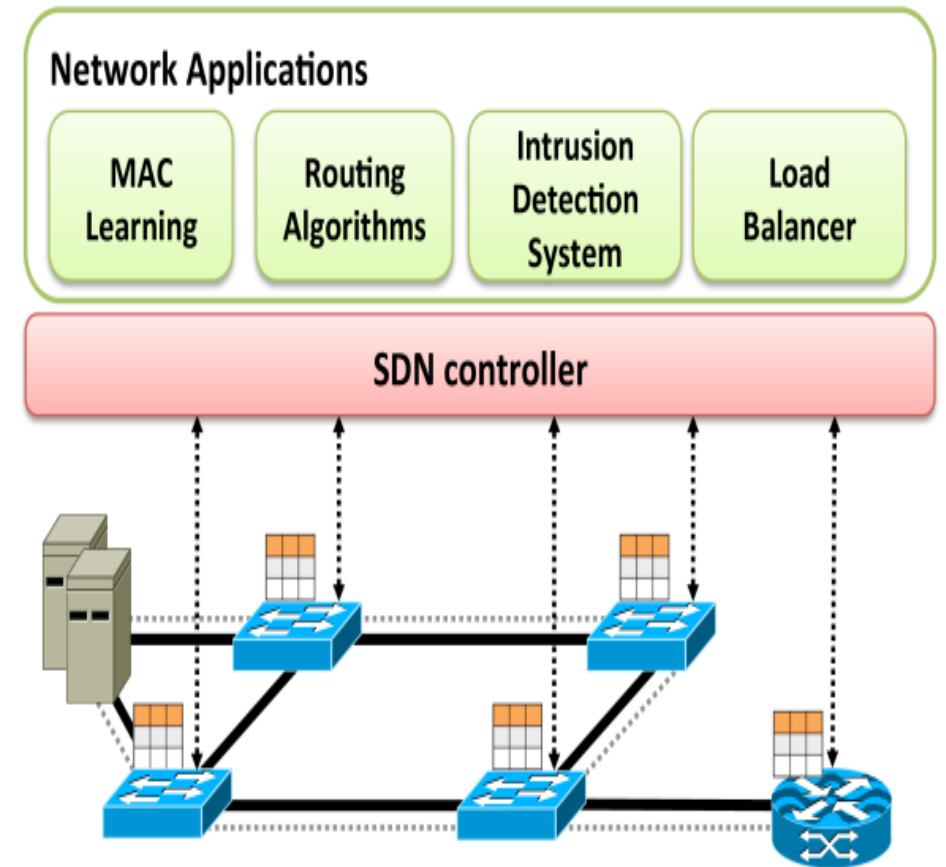
SDN Use Cases

❑ Security Enhancement in SDN

- ❖ In traditional architectures, we need to monitor as many network links as possible.
- The source of attacks is unknown (e.g., botnets).
- ❖ The centralized controller's global view in SDN facilitates attack detection.
- instructing network devices to pass the flow traffic to the controller for further inspection without installing additional equipment.
- In terms of any suspicious traffic patterns, the controller generates alerts and instructs the SDN switches to block the source.

❑ SDN Traffic Management

- ❖ The quality of service (QoS) has been commonly applied in the traditional network, which faces many difficulties in guaranteeing the QoS for different applications.
- ❖ The SDN network's global view facilitates the configuration of the QoS since SDN simplifies system management through the efficient use of resources.



SDN Security Challenges

- ❖ The new features of SDN can generate new security issues.
- ❖ The security breach in the conventional networks has limited damage for only a small part of the network.
i.e. probably for the same network vendor.
- ❖ All SDN layers can be compromised to various sources of attacks.
- ❖ These attacks become more dangerous if they target the SDN controller.
- ❖ In case the attacker gains access to the SDN controller, he can drop all incoming traffic or redirect it.

One of the most dangerous attacks in SDN is Denial of Service (DoS) , or even worse Distributed Denial of Service (DDoS).

- ❖ A significant increasing in the use of ML/DL techniques to address the requirements for developing powerful IDSs.

- ❖ **My research focuses on developing a novel anomaly detection approach aimed to improve the detection accuracy and efficiency of the IDS, which is essential for SDN security.**

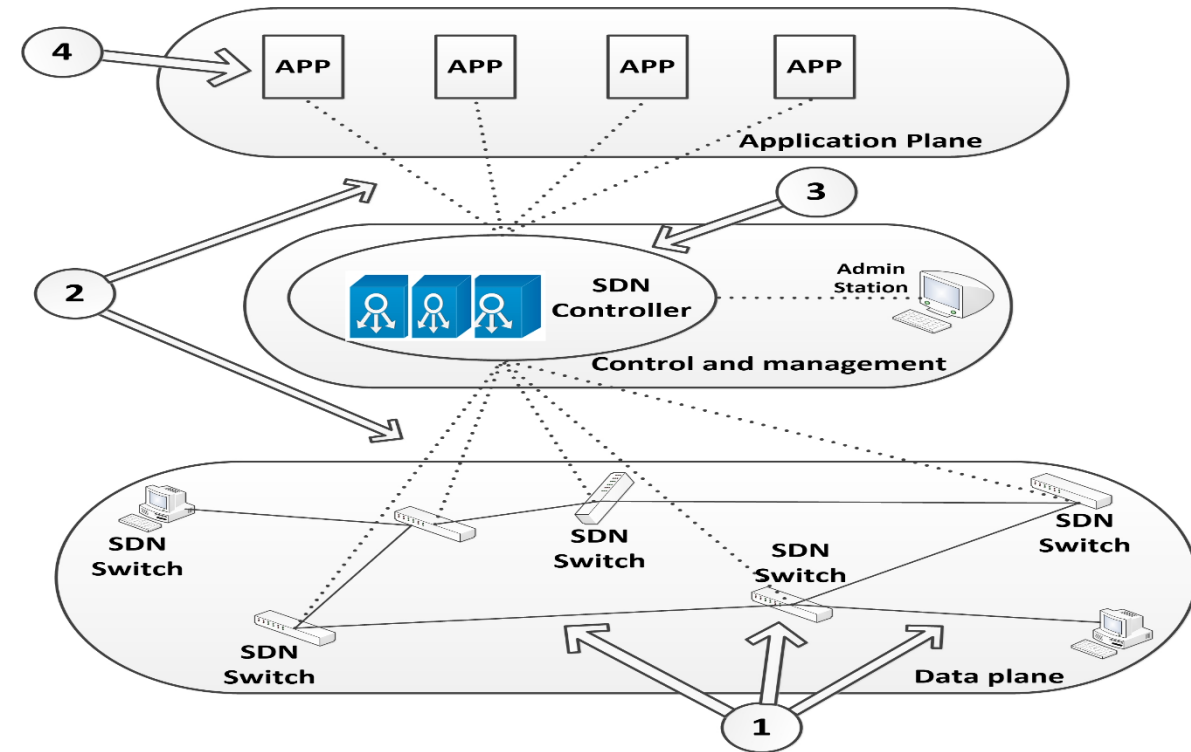


Figure: SDN main threat vectors map.

SDN Security Challenges

DDoS Attack Case Study

- ❖ The new architecture of SDN (i.e., decoupling the data plane from the control plane) creates DDoS attack surfaces that did not exist in conventional networks.
- ❖ The SDN controller becomes a single point of failure and a prime target for attackers to exploit.
- ❖ Hping3 tool is used to flood the victim server and send the attack packets.
- ❖ The experiment test is measured for 60 s, and the DDoS flooding attacks last for 10 s.
- ❖ Studying DDoS attacks' effects and their consequences on the SDN controller's load and throughput.

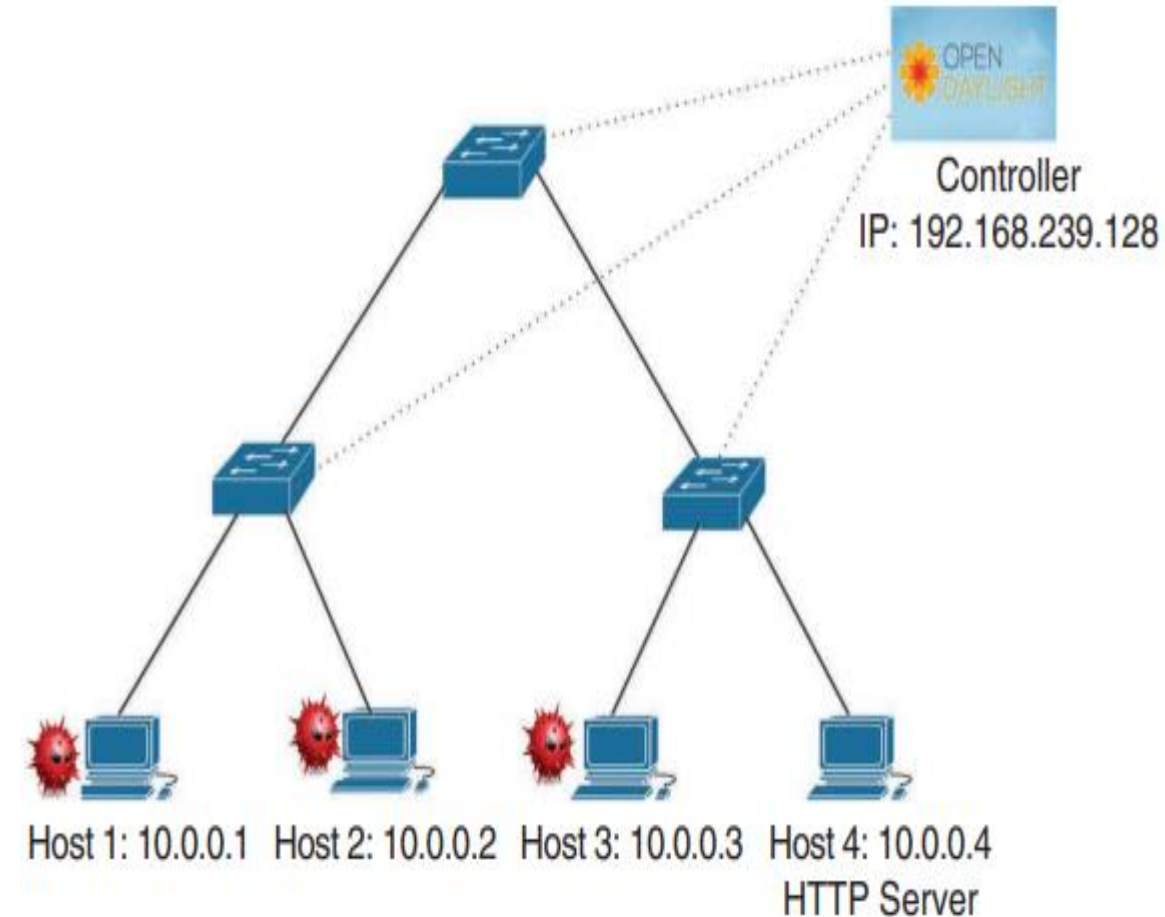


Figure: The network topology

SDN Security Challenges

The experiment Results

- ❖ Before the attack, the controller load and the network throughput are low.
- ❖ During the attack, there is a significant increase in the CPU load due to the flooding attacks.
- ❖ the controller is flooded with many requests, raising the throughput and eventually exhausting and plunging the controller.

The overall conclusion is that

- ❖ An attacker controlling a few hosts can completely exhaust the network resources or degrade the system's performance.
- ❖ Enhancing the security of the controller is an essential issue in the SDN system.

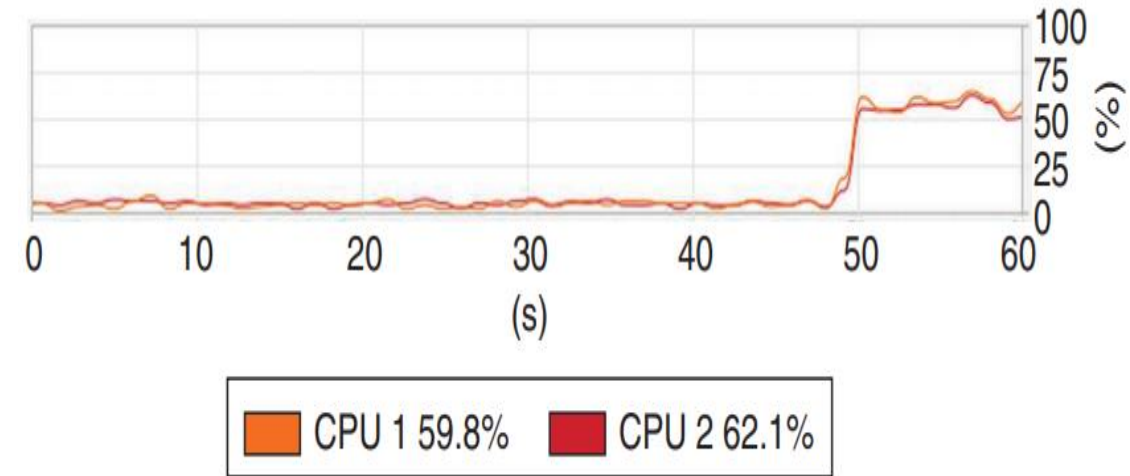
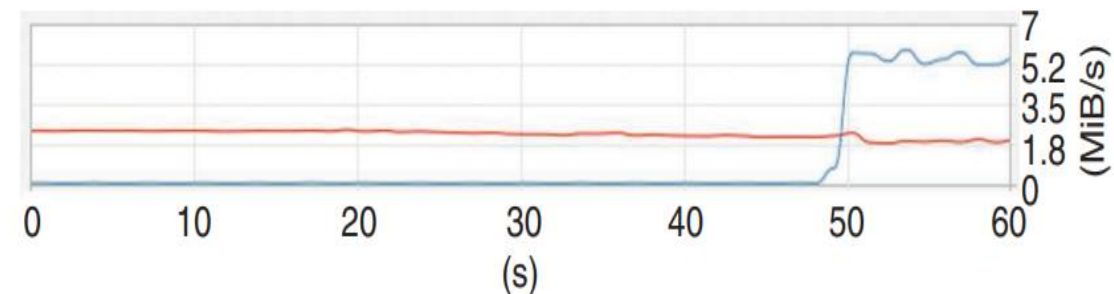


Figure: The CPU load before and after DDoS flooding attacks



↓ Receiving	5.4 MiB/s	↑ Sending	2 MiB/s
Total Received	46.3 GiB	Total Sent	3 GiB

Figure: The network throughput before and after DDoS flooding attacks.

Defense Mechanism in the SDN

Several traditional methods have been proposed to detect malicious behaviour in networks

- ❖ Threshold analysis methods

- ❖ Statistical methods

- ❖ Signature methods

- Unfortunately, these methods rely on the security researchers experience to quantify the malicious traffic behaviour based on the past observation.
- For example, selecting a sub-optimal threshold value for any network system may not be reliable or being easy to identify.
- It often takes a long time to monitor network traffic in real time in order to find out the optimal threshold value.

- ❖ The last decade has witnessed a significant increasing in the use of machine learning (ML) and deep learning (DL) techniques to address the requirements for developing powerful Anomaly Detection techniques.

Anomaly via Intrusion

What is an Anomaly?

- Is it the sleeping dog, because all the others are awake?
- Is it the dog with the very long fur?
- Is it the dog with balls in his mouth, or the one with a tongue hanging out?

There could be many answers to the question.

Depending on what criteria are used to define an anomaly



Anomaly via Intrusion

Anomaly Background

- ❑ “Anomaly is a pattern in the data that does not conform to the expected behaviour” [1]
- ❑ Notion of anomaly depends on application domain and context.
- ❑ Examples
 - Network monitoring – network traffic, performance indices and logs are monitored to **detect failures in the network**
 - Fraud detection – log data is analysed, to detect misuse of a system, for example, financial transactions to **detect credit card fraud**
 - Medical applications – patient monitoring, where ECG or other body sensors are logged and analysed to detect critical or **life-threatening situations**
 - Video surveillance – camera data is analysed for **suspicious movements**
- ❑ • **Intrusion detection – network traffic and server applications are monitored to detect potential intrusion attempts**
- ❑ The anomaly detection techniques can be categorized into two main approaches: **statistical and machine learning approaches.**

[1] Chandola, Varun, Arindam Banerjee, and Vipin Kumar. "Anomaly detection: A survey." ACM Computing Surveys (2009)

Anomaly Based Solutions in SDNs

Shortages of ML Approaches

- ❖ The ML-based techniques have shortages in detecting the attacks that have never seen before.
- ❖ Most of the work that deploys ML approaches is heavily based on feature engineering.
- ❖ It is both cumbersome and error-prone to manually handcraft and extract the discriminatory features from the network traffic.
- ❖ The majority of the real-world data takes the approach of non-linear or multivariate data. However, ML algorithms have a poor ability to learn the complex and non-linear structure of the data.

Anomaly Based Solutions in SDNs

DL for Cybersecurity Tasks

- ❖ On the other hand, DL is considered one of the most significant solutions to solve the weaknesses of ML algorithms
- ❖ In recent years, many companies, such as Google, Microsoft, and Facebook, are broadly used DL in different applications i.e. speech recognition and image processing.
- ❖ The vital part of DL techniques is to extract the intensive features automatically from raw data records.
- ❖ DL can address large-scale network traffic using multiple processing layers to find a good representation of the input data, which is generally hard to obtain using traditional methods.
- ❖ Nowadays, DL algorithms such as RNN, Deep Autoencoders (DAE), and Convolutional Neural Network (CNN) attract the attention of research community and become a promising research topic for dimensionality reduction issues.
- ❖ Therefore, it can be applied in many cybersecurity tasks such as intrusion detection, traffic analysis, it can impact the robustness of the anomaly detection system and lead to poor model performance for zero-day attacks.

Visual Abstract of the Flow-based Anomaly detection in SDN

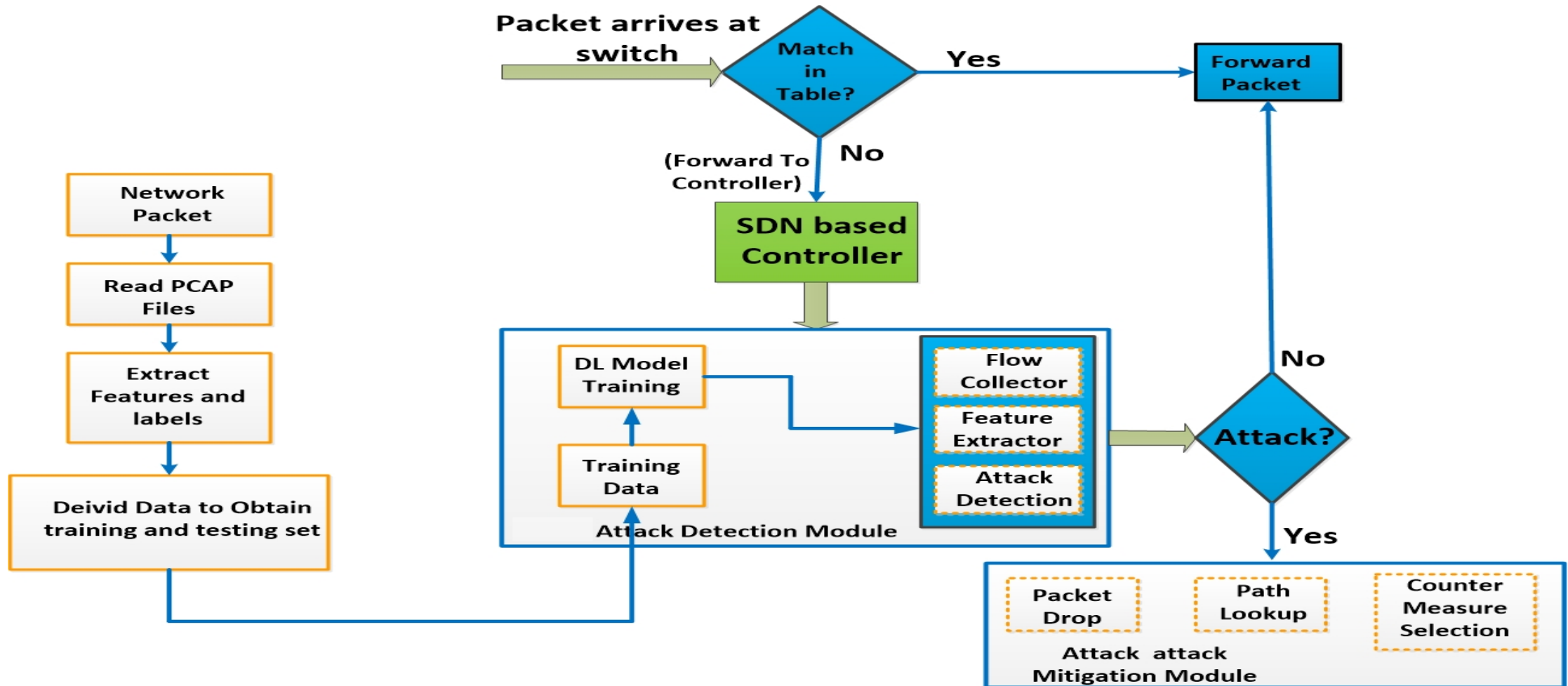


Figure: Anomaly detection and mitigation Framework in SDN.

Contributions

SDN Dataset Preparation.

- ❖ Proposing a virtualised network test-bed to generate a new SDN dataset, namely InSDN.
- ❖ Generating a significant dataset covers various attacks that can be found in all SDN elements from the proposed network testbed.
- ❖ Review the impact of the generated attacks on the different elements of SDN.
- ❖ Demonstrating how to use the new dataset with popular ML techniques applied in anomaly detection systems for the SDN network.

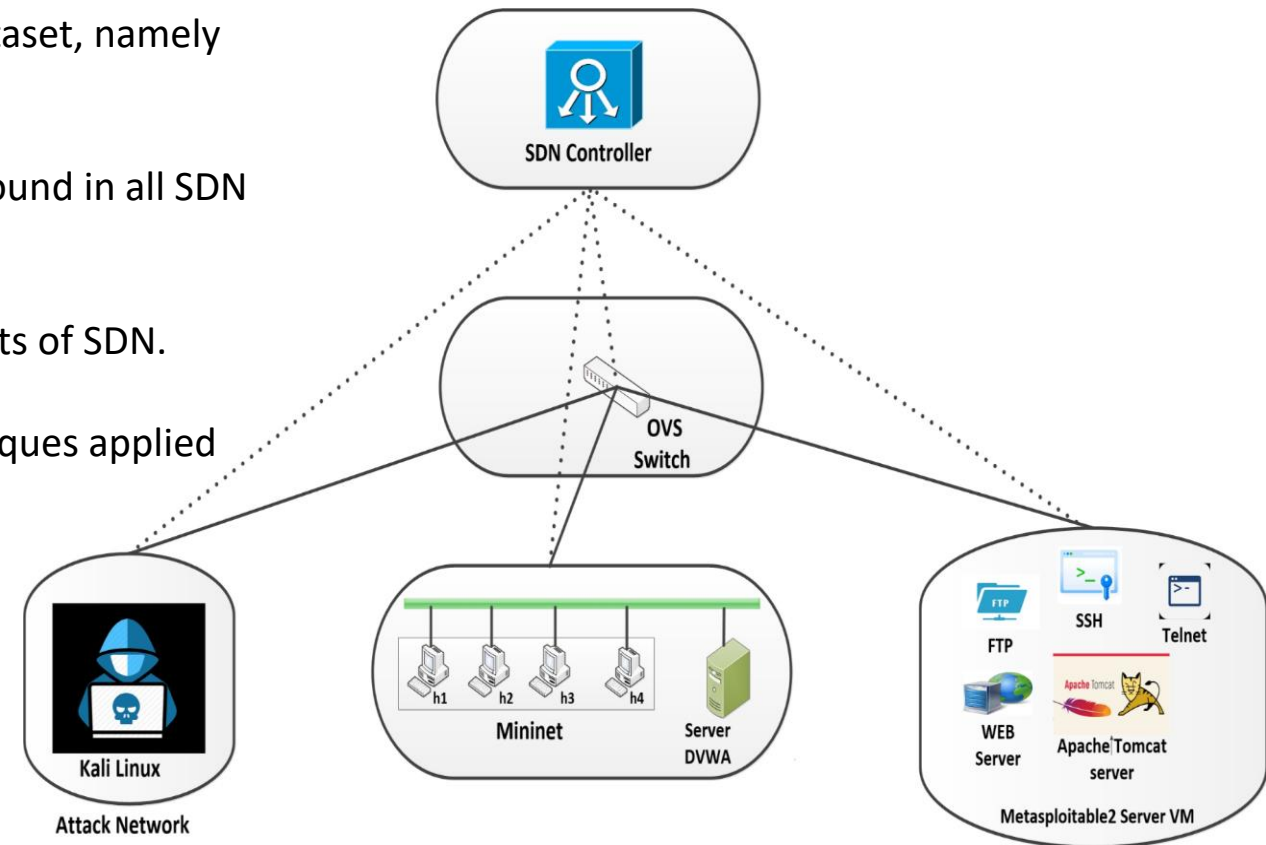


Figure: Virtual SDN testbed network architecture. The Virtual topology was created using four separated VM machines. The OVS switch and SDM controller were installed on two different machine, while the Kali Linux and Metasploitable 2 are representing the attacker machine and the vulnerable Linux server respectively.

Contributions

A DL approach against DDoS Attacks.

- ❖ Develop a lightweight IDS approach with minimum features without deteriorating the IDS performance.
- ❖ A DL approach (i.e. DDoSNet) based on LSTM and Autoencoder against DDoS attacks in SDN.
- ❖ Find the most relevant DDoS attack features in each dataset individually using two popular feature selection methods (IG and RF).
- ❖ Three benchmark flow based datasets i.e. InSDN , CICIDS2017 and CICIDS2018 were used for our analysis .

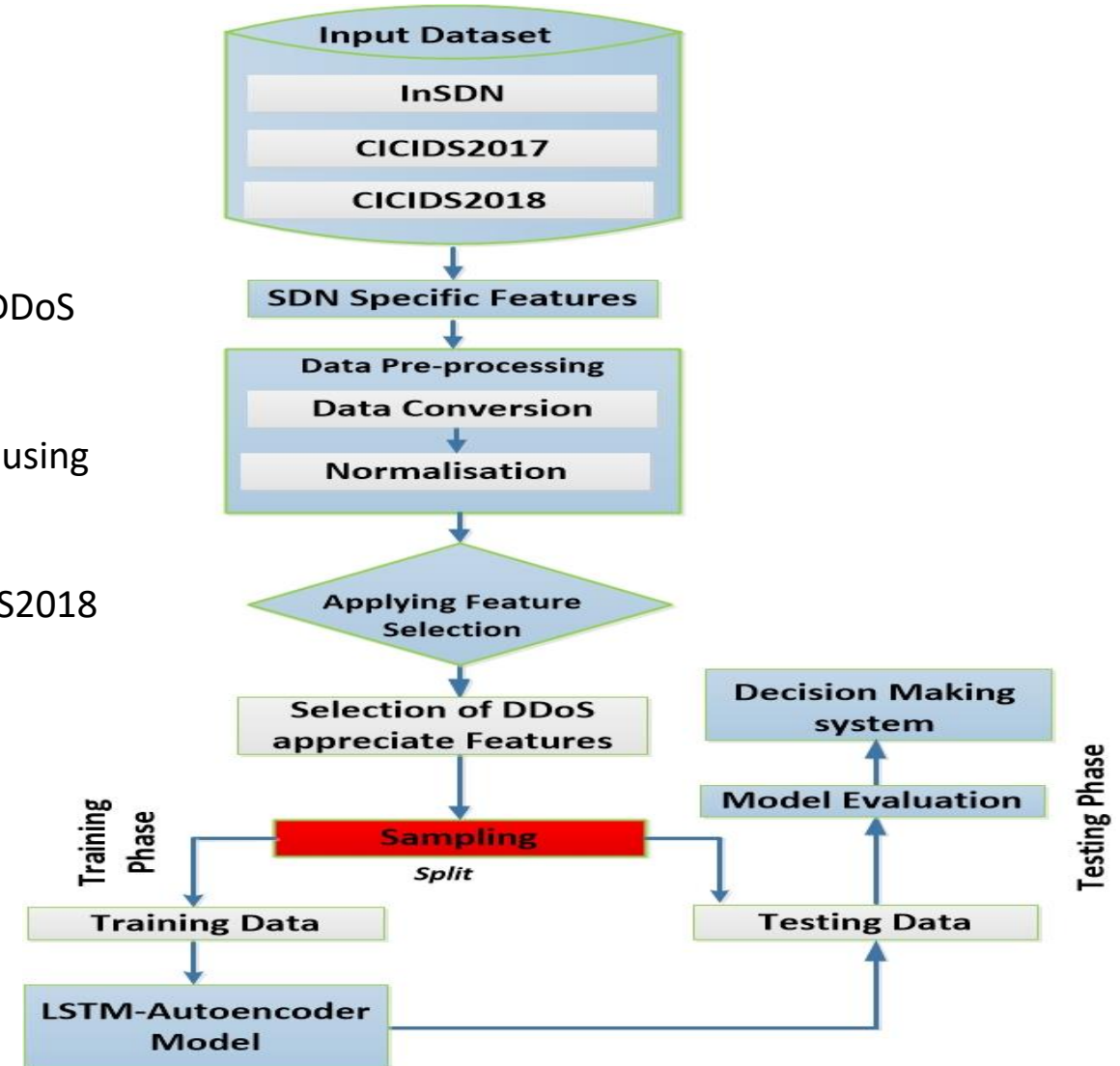


Figure: The flow diagram of the DDoS Detection module

Contributions

An Improved CNN Learning Approach for IDS in SDNs.

- ❖ Solve the problem of overfitting, resulting from the noisy data.
- ❖ SD-Reg is implemented to overcome this constraint that considers the weight values' dispersion, known as the standard deviation.
- ❖ We minimise the loss function concerning w by a standard deviation to adopt values within a specific range.
- ❖ The regulariser prevents the learning model from taking wide spread values from the weight space.

$$\text{Cost function} = \text{Loss} + \lambda \sigma(w)$$

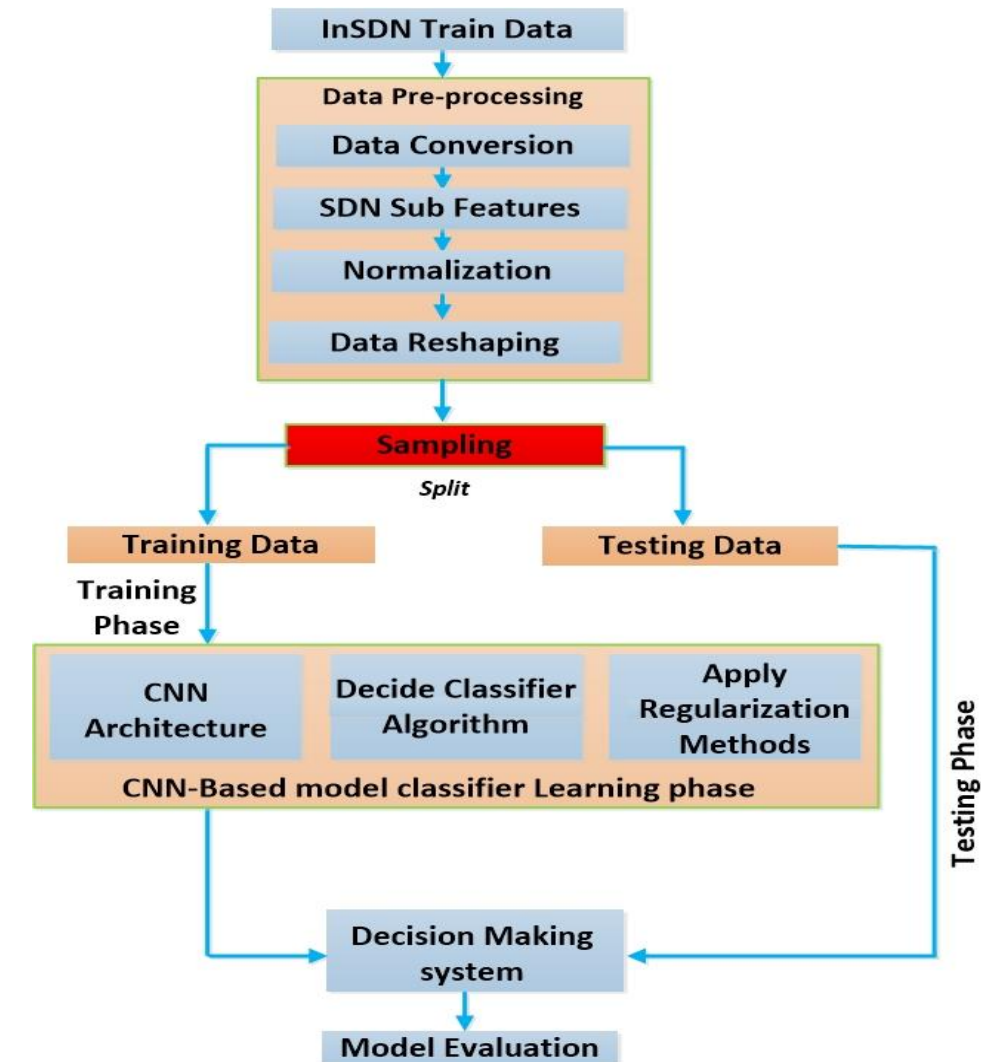


Figure: The diagram flow of the proposed method

Contributions

An Anomaly Detection Technique for Unlabeled and Imbalanced Dataset.

- ❖ Dealing with highly unbalanced and unlabeled data, which cause the detection approach strongly biased to some of the classes.
- ❖ The One-Class SVM algorithm is integrated with the LSTM-Autoencoder to better characterise the network traffic; hence, the detection rate can significantly improve.
- ❖ The model was trained using only samples from the normal data, and then it was applied for a new testing data, which included both normal and malicious traffic.

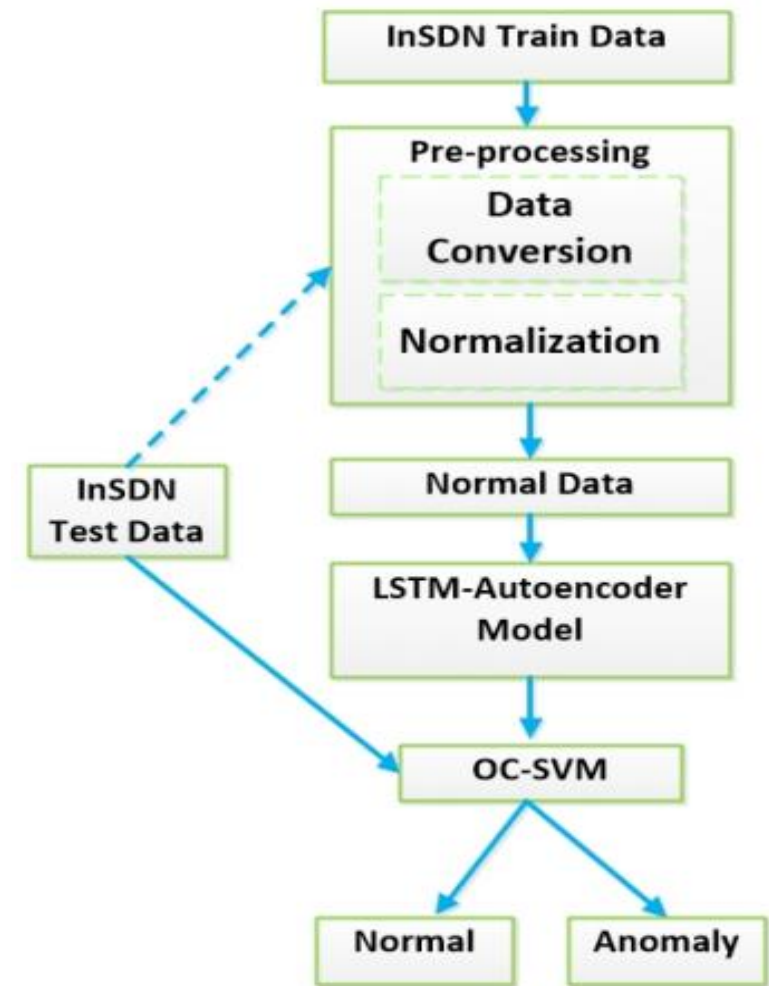


Figure: The diagram flow of the proposed method using - InSDN data set.

Defense-in-Depth

- ❖ It is very important to highlight about the question, How Secure is Secure Enough?
 - many articles scattered over a long time span with this question title.
- ❖ Unfortunately, there is no 100% security since we can not cover all the risks, even all the risks we identify in an organisation.
 - Measure and evaluate the business impact that those identified risks could potentially pose.
 - Then, prioritise the business impact of not mitigated incidents.
- ❖ The answer of the aforementioned question requires all the stakeholders in the company be involved in the decision-making process.
- ❖ It transforms to another type of question like what security standards does the company specifically require to certify?
 - will go with one of the security standards, such as ISO 27001, TISAX (stands for Trusted Information Security Assessments Exchange).
- ❖ As a result, they will have a clear cut how the company's budget is measured and planned to be spent on security requirements of the organisation.

Looking Ahead

Based on the findings of this work, several future directions can be identified.

- ❖ Extend the work of the dataset and create a more intrinsic dataset generated from large-scale networks.
 - consider several controllers in the new test-bed and study the impact of the attacks for each controller to find the suitable security measurements.
 - Consider new attack categories for the best representative of existing real-world networks
- ❖ Deploy the developed model under SDN context in one or more realistic network settings.
 - determine how DL might be applied in practice, and how well it would perform in real-world scenarios.

List of Publications

Journal Papers :

- [1] M. S. Elsayed, N.-A. Le-Khac, and A. D. Jurcut, "Insdn: A novel sdn intrusion dataset," Journal of IEEE Access, vol. 8, pp. 165 263–165 284, 2020.
- [2] M. S. Elsayed, N.-A. Le-Khac, M. A. Albahar, and A. D. Jurcut, "A novel hybrid model for intrusion detection systems in sdns based on cnn and a new regularization technique," Elsevier - Journal of Network and Computer Applications, vol. 191, p. 103160, 2021.
- [3] M. S. Elsayed, N.-A. Le-Khac, M. AZER, and A. D. Jurcut, "A flow based anomaly detection approach with feature selection method against ddos attacks in sdns," Journal of IEEE transactions on cognitive communications and networking, Under Press.

Magazine Papers:

- [4] M. S. Elsayed, N.-A. Le-Khac, and A. D. Jurcut, "Dealing with covid-19 network traffic spikes," IEEE Security & Privacy magazine [cybercrime and forensics], vol. 19, no. 1, pp. 90–94, 2021.

Conference Papers

- [5] M. S. Elsayed, N.-A. Le-Khac, S. Dev, and A. D. Jurcut, "Machine-learning techniques for detecting attacks in sdn," in 2019 IEEE 7th International Conference on Computer Science and Network Technology (ICCSNT), Dalian - China. IEEE, 2019.

List of Publications

Conference Papers-continue

- [6] M. S. Elsayed, N. A. Le-Khac, S. Dev, and A. D. Jurcut, "Ddosnet: A deep-learning model for detecting network attacks," in 2020 IEEE 21st International Symposium on "A World of Wireless, Mobile and Multimedia Networks"(WoWMoM), Cork, Ireland. IEEE, 2020, pp. 391–396.
- [7] M. S. Elsayed, H. Z. Jahromi, M. M. Nazir, and A. D. Jurcut, "The role of cnn for intrusion detection systems: An improved cnn learning approach for sdns," in International Conference on Future Access Enablers of Ubiquitous and Intelligent Infrastructures, Zagreb - Croatia. Springer, 2021, pp. 91–104.
- [8] M. S. Elsayed, N.-A. Le-Khac, H. Z. Jahromi, and A. D. Jurcut, "A hybrid cnn-lstm based approach for anomaly detection systems in sdns," in The 16th International Conference on Availability, Reliability and Security, Vienna - Austria, 2021, pp. 1–7.
- [9] M. S. Elsayed, N.-A. Le-Khac, S. Dev, and A. D. Jurcut, "Detecting abnormal traffic in large-scale networks," in 2020 International Symposium on Networks, Computers and Communications (ISNCC), Montreal - Canada. IEEE, 2020, pp. 1–7.
- [10] M. S. Elsayed, N. A. Le-Khac, S. Dev, and A. D. Jurcut, "Network anomaly detection using lstm based autoencoder," in Proceedings of the 16th ACM Symposium on QoS and Security for Wireless and Mobile Networks. Alicante - Spain, 2020, pp. 37–45.

Thank You

Email: anca.Jurcut@ucd.ie