Peer-to-Peer Networking and Applications (2019) 12:493–501
https://doi.org/10.1007/s12083-017-0630-0

Survey on SDN based network intrusion detection system using machine learning approaches

Nasrin Sultana[1] · Naveen Chilamkurti[1] · Wei Peng[2] · Rabei Alhadad[1]

Received: 29 July 2017 / Accepted: 26 December 2017 / Published online: 12 January 2018

Abstract
Software Defined Networking Technology (SDN) provides a prospect to effectively detect and monitor network security problems ascribing to the emergence of the programmable features. Recently, Machine Learning (ML) approaches have been implemented in the SDN-based Network Intrusion Detection Systems (NIDS) to protect computer networks and to overcome network security issues. A stream of advanced machine learning approaches – the deep learning technology (DL) commences to emerge in the SDN context. In this survey, we reviewed various recent works on machine learning (ML) methods that leverage SDN to implement NIDS. More specifically, we evaluated the techniques of deep learning in developing SDN-based NIDS. In the meantime, in this survey, we covered tools that can be used to develop NIDS models in SDN environment. This survey is concluded with a discussion of ongoing challenges in implementing NIDS using ML/DL and future works.

Keywords NIDS · Machine learning · Deep learning · SDN

1 Introduction

Network Intrusion Detection systems (NIDS) have been developed rapidly in academia and industry in response to the increasing cyber-attacks against governments and commercial enterprises globally. The annual cost of cybercrime is continuously rising [1]. The most devastating cyber crimes are those caused by malicious insiders, denial of services and web-based attacks. Organizations can lose their intellectual property with such malicious software crept into the system which may lead to disruptions to a country's critical national infrastructure. Organizations deploy a firewall, antivirus software, and an intrusion detection system (NIDS) to secure computer systems from unauthorised access [3].

One of the focused areas to resolve cyber-attacks quickly is to detect the attack process early [1] from the network using NIDS. Network intrusion detection systems (NIDS) are designed to detect malicious activities including virus, worm, DDoS attacks. The critical success factors for NIDS are abnormality detection speed, accuracy and reliability. Machine learning techniques (ML) is applied to develop NIDS to improve detection accuracy [5] and low false alarm rate [4]. As an advanced stream of ML, deep learning (DL) approaches have been adopted in the field of NIDS. The recent development focuses on leveraging a new network architecture, namely, the software-defined network (SDN) to implement NIDS with machine learning approaches [6].

Software-defined network is an emerging architecture that decouples network control and forwarding functions so that the network control can be directly programmable [7]. The segregation of the control plane from the data plane enables easy network management [2]. This feature of SDN is facilitating

This article is part of the Topical Collection: *Special Issue on Software Defined Networking: Trends, Challenges and Prospective Smart Solutions*
Guest Editors: Ahmed E. Kamal, Liangxiu Han, Sohail Jabbar, and Liu Lu

✉ Naveen Chilamkurti
n.chilamkurti@latrobe.edu.au

Nasrin Sultana
n.sultana@latrobe.edu.au

Wei Peng
w.peng@latrobe.edu.au

Rabei Alhadad
r.eludad@latrobe.edu.au

[1] Department of Computer Science and IT, La Trobe University, Melbourne, Australia

[2] Department of Accounting and Business Analytics, La Trobe University, Melbourne, Australia

innovative applications, dictating a new networking paradigm capable of implementing NIDS [9]. Machine learning and deep learning (ML/DL) approaches can be implemented in the SDN controllers to enhance network monitoring and security [6].

Several research works have been done to implement NIDS, with integrated deep learning algorithms using SDN controller before. In [6], the authors integrated anomaly algorithm in to open flow switches using a controller. They constructed a deep neural network to simplify the features of normal and abnormal traffic. To evaluate their model, they also implemented deep learning algorithms. In [8], the authors proposed an SDN based DDoS detection system comprises of three modules. The three modules are implemented on the top of the controller and deep learning approach was used for feature extractor and traffic classification. In [38], the authors proposed a lightweight DDoS flooding attack detection solution, which uses emulation to build a NOX based network in SDN using self-organized map (SOM).

There are many review papers covering ML/DL methods in various domains. Little has been done around NIDS based on SDN. We focus on depicting SDN as a platform for implementing NIDS with ML/DL approaches beyond the reach of existing review works.

The remainder of this paper has organized as follows: Section 2 introduces NIDS followed by a general discussion of ML approaches and subsequently ML/DL based NIDS observation. Section 3 provides an overview of SDN architecture and applications. We also review SDN-based NIDS implementation and observation. In Section 4, research challenges associated with applying to ML/DL to SDN-based NIDS are discussed. Section 5 concludes the paper with future works.

2 Network intrusion detection system (NIDS) and evaluation

An Intrusion Detection System (IDS) is developed in a network to detect threats from monitoring packets transmitted though. IDSs detect anomalous and malicious activities from inside and outside intruders [10]. An IDS need to deal with problems such as vast network traffic volumes and highly uneven data distribution.

The primary function of an IDS is to monitor information sources, such as computers or networks, for unauthorised access activities. IDSs collect data from different systems and network sources and analyse the data for possible threats [10]. IDSs are further developed into network intrusion detection systems (**NIDS**) and host-based intrusion detection systems (HIDS). Figure 1 shows a general overview of IDSs based on the implemented detection techniques and the deployment environment.

As shown in Fig. 1, intrusion detection system can be implemented using different methods and techniques. A number of detection mechanisms have been developed to detect abnormalities, which are categorized into statistical methods, data-mining methods and machine learning based methods [11]. NIDS can be implemented using three detection techniques: the signature based detection and the anomaly based detection [33]. A signature based NIDS is limited to detecting from known malicious threats. A combination of the packet header and packet content inspection rules are applied to the detection system from the anomalous traffic flows through signature specification. Anomaly detection techniques are designed to automatically understand attacks which are unknown and unpredictable for signature-based NIDS [11]. Machine learning methods are one of the examples of anomaly based intrusion detection techniques.

There are some evaluation criteria to compare the performance of algorithms in NIDS such as accuracy, false negative rate (FNR), false positive rate (FPR), time used, memory consumption and kappa statistics [33]. Accuracy, FNR and FPR are often used as evaluation criteria for the NIDS [33]. A comparison of three detection method based on different performance criteria for NIDS shown in Table 1.

We focused on reviewing the state-of-the-art machine learning algorithms in implementing NIDS in this section.

2.1 Machine learning in network intrusion detection system

The domain of Machine learning (ML) is dedicated to developing systems that can automatically learn from the data [12] and identify hidden patterns without being explicitly programmed to do so [10]. ML algorithms is categorized by the learning style they employ and by the functional similarity of how they work [10]. Figure 2 presents an overview of machine learning approaches based on their learning styles. Machine learning techniques are regarded as efficient methods to improve detection rate, reduce false alarm rate, and in the meantime, decrease computation and communication cost [13].

The machine learning approaches can be categorized into supervised, unsupervised learning and semi-supervised learning [3].

In supervised learning, the algorithms learn representations from labelled input data to predict unknown cases. Examples of supervised machine learning algorithms are support vector machine (SVM) for classification problems and random forest for classification and regression problems [12].

Support vector machine (SVM) algorithms are widely used in NIDS research due to its powerful classification power and practicality in computation. They are suitable for high dimensional data, but selecting a reasonable kernel function is critical. It is resource hungry, demanding computational processing units and memory [10]. The Random forest algorithm [14] as a powerful ensemble supervised learning approach to deal effectively with uneven data, however it is subjective to over-fitting.

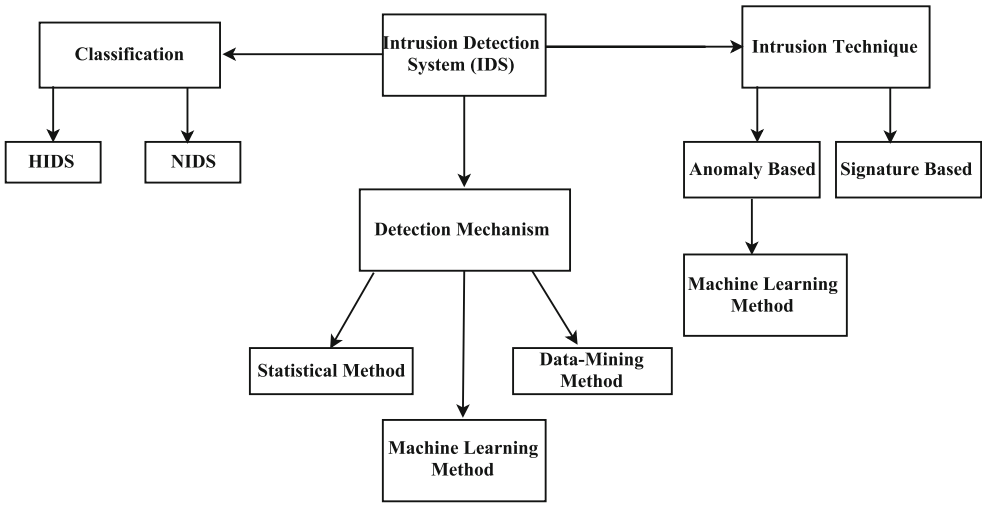

Fig. 1 Overview of intrusion detection system

In the unsupervised learning scheme, the algorithms learn the structure and representations from unlabeled input data. The goal of an unsupervised learning algorithm is to model the fundamental structure or distribution in the data to predict unknown data [12]. Examples of unsupervised learning algorithms are feature reduction techniques like principal component analysis (PCA) and clustering techniques, for example, self-organizing map (SOM).

Principal Component Analysis (PCA) is an algorithm that is used to significantly speed up unsupervised feature learning [32]. Many researchers use PCA for feature selection before applying classification [15]. The clustering algorithms such as K-means and other distance-based learning algorithms are used for anomaly detection. A self-organizing map (SOM) is an artificial neural network that was used to reduce payload in NIDS [16]. The disadvantage of using clustering algorithms in anomaly detection is that the clustering algorithms are subjective to initial conditions, for example centroid and may produce high false positive rate [17].

Semi-supervised learning is a type of supervised learning that also use unlabeled data for training. The training data consist of a small amount of labeled data and a large number of unlabeled data. It is suitable for circumstances when large amounts of labelled data are unavailable, for example, photo archives where only some of the images are labelled (e.g. a person) and most of them are unlabeled [18]. The Semi-supervised support vector machine [19], was used to enhance the accuracy of NIDS [20]. Two semi-supervised classification method Spectral Graph Transducer and Gaussian Fields approach, used to detect unknown attacks and one semi-supervised clustering method MPCK-means used to improve the performance of the detection system [21].

Deep Learning algorithms are a modern update to artificial neural networks that exploit abundant, affordable computation [22]. Deep learning permits an algorithm to learn representation of data with various levels of generalization. These methods have been applied to visual object recognition, object detection, detecting network intrusion and many other domains [23]. A deep learning algorithm can be trained as a supervised and unsupervised way [12].

Deep Learning algorithm in a supervised way**:** Convolutional neural network (CNN) [23] is normally trained in a supervised way. CNN is now the benchmark model for the computer vision purpose. The CNN architecture used to structure 2D images [24] and a most important acknowledgement of CNN is face recognition [23].

- Deep Learning algorithm in an unsupervised way: An autoencoder [25] is used to learn a representation (encoding) for a set of data for the purpose of dimensionality reduction. A Deep Belief Network (DBN) [26] can learn to reconstruct its inputs when trained with a set of examples in an unsupervised way. The layers then act as feature detectors on inputs. After this learning step, a DBN is further trained in a supervised way to perform classification. DBNs, such as restricted Boltzmann machines

Table 1 Comparison detection method [33]

Detection technique	Alarm Rate	Speed	Flexibility	Reliability	Scalability	Robustness
Signature	Low	High	Low	High	Low	Low
Anomaly	High	Low	High	Moderate	High	High

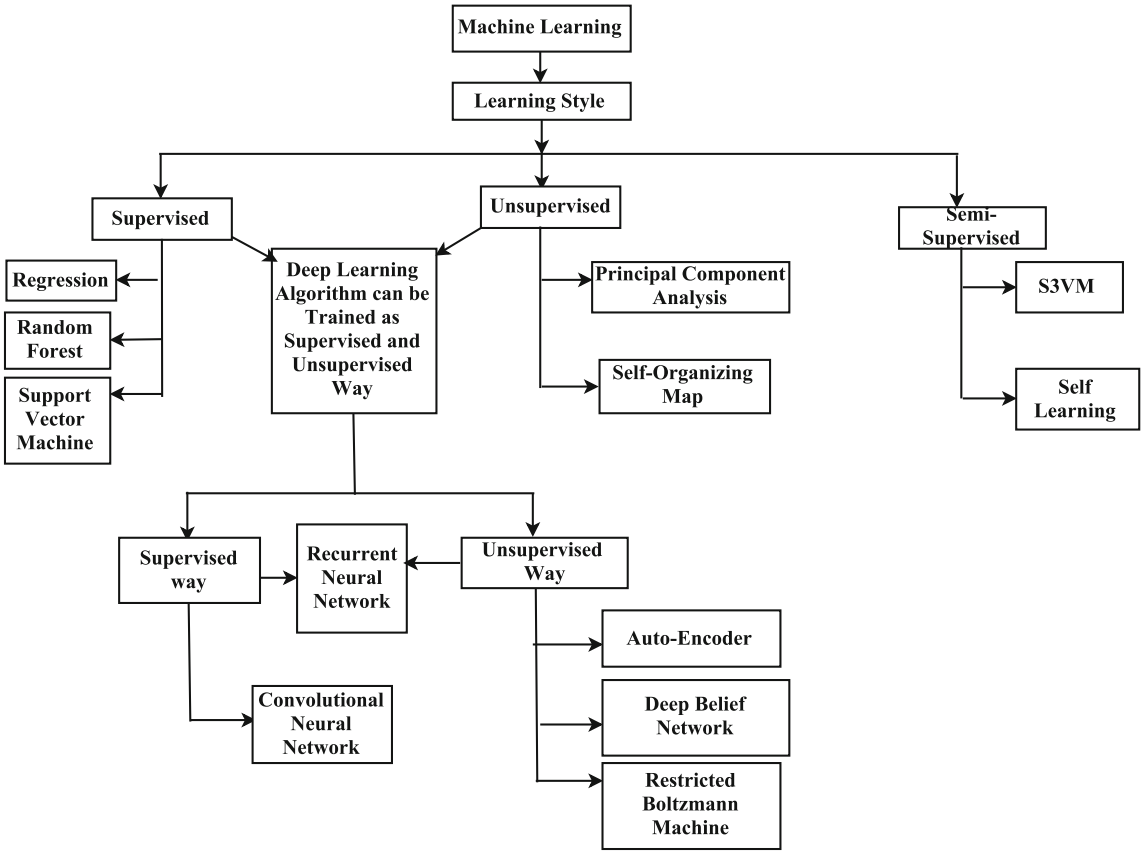

Fig. 2 Overview of machine learning approaches

(RBMs) [27] or auto-encoders apply to dimensionality reduction, regression, collaborative filtering, feature learning and topic modelling, etc.

- Deep Learning algorithm in a supervised or unsupervised way: Recurrent neural network (RNN) [28] algorithms are considered as a supervised or unsupervised learning method. RNNs can leverage internal memory to process random orders of inputs. Speech recognition is a typical application for RNN [29]. RNN is good at prediction of character in the text and also can learn dependencies and actual evidence which is stored for a long time [23].

2.2 ML-based NIDS observation

ML/DL techniques have been used to develop NIDSs, such as Artificial Neural Networks (ANN), Support Vector Machines (SVM), Naive-Bayesian (NB), Random Forests (RF), self-organizing map (SOM) etc. [15]. [30] implemented a NIDS based on a restricted Boltzmann machine (RBM) for feature reduction and a support vector machine (SVM) for classification. The accuracy of the system is approximately 87%. [31] developed a network anomaly detection system using discriminative RBM in conjunction with generative models with good classification accuracy abilities to gather knowledge from training data.

ML/DL Approach used for NIDS: In [14], eight tree based classification algorithms are evaluated in predicting network events. The decision tree algorithm is used for feature selection and a random forest algorithm is applied as a classifier for NSL-KDD dataset. [33] deployed a principal component analysis (PCA) algorithm for feature selection and a support vector machine as a classifier to select the optimum feature subset. [15] implemented flexible NIDS using self-taught learning on NSL-KDD data for network intrusion and developed a sparse encoder for further reduction. They also used soft-max regression as a classifier and evaluated their model independently on training and test datasets with an accuracy on training data 92.48%. Most of the approaches used training data for both training and testing purpose, [15] used separate training and testing data for training and testing which provides accuracy of detection techniques. [31], experimented that if they tested their proposed classifier in different training data, performance degraded. [14], experiments showed a random tree model holds the high accuracy and low false alarm rate in detection system as a classifier.

3 Software-defined networking (SDN) based NIDS

One of the features in the Software-Defined Networking (SDN) architecture is the separation of control plane to data plane, which makes packet forwarding simple [2]. The centralized controller of SDN has the real-time feedback control capability [34], and open interfaces which offer modular plug-in features. The centralized controller provides an abstract network view, defining tasks by APIs and greater programmability of the network [9]. It can integrate security devices within the network topology [35], which can lead to increase in accuracy, detecting security incidents and simplify management.

In this section, we first introduce the architecture of SDN and applications, followed by SDN-Based NIDS observation using ML/DL.

3.1 SDN architecture and applications

Open Networking Foundation (ONF) [7] is one of the suitable architecture for SDN; it is divided into three main functional layers. These are infrastructure layer, control layer, and application layer. Figure 3, illustrate the overview of SDN architecture, as shown in Fig. 3, the upper layer is the application layer; the control plane is in the middle and data plane is the lower layer which is also known as infrastructure layer.

1) **Infrastructure Layer:** Infrastructure layer is also known as data plane. It mainly consists of forwarding devices (FEs) including physical switches which interconnected through wired or wireless media. Examples of physical switches are Juniper, HP etc. and virtual switches such a OpenvSwitch.
2) **Control Layer:** Control layer is also known as the control plane; it consists of a set of software-based SDN controllers providing a combined control functionality through open APIs to supervise the network forwarding behavior through a public interface. Three communication interfaces allow the controllers to interact: southbound, northbound and east/westbound interfaces. Southbound APIs achieves communication between the controller and the physical networking hardware. SDN North Bound Interfaces (NBI) communicate between SDN application and control layer that provide general network overviews. The east-westbound interfaces using mainly to communicate between controller to expand controls within a domain.
3) **Application layer:** The upper layer, application layer consists of the end user business application such as network monitoring and security applications.

Using extended features of SDN, number of SDN applications have been developed to increase flexibility of a network, reduce the total time to market and total cost of ownership of future IT network infrastructures. SDN has found applications in a wide range of networking avenues. Furthermore, due to the recent increase in the number of cyber-attacks, SDN architecture has been used for rapid development and deployment of new services. In this section, some of the key applications of SDN are discussed [36].

- **Wireless Communication:** The programmability feature of SDN paradigm introduces new applications to

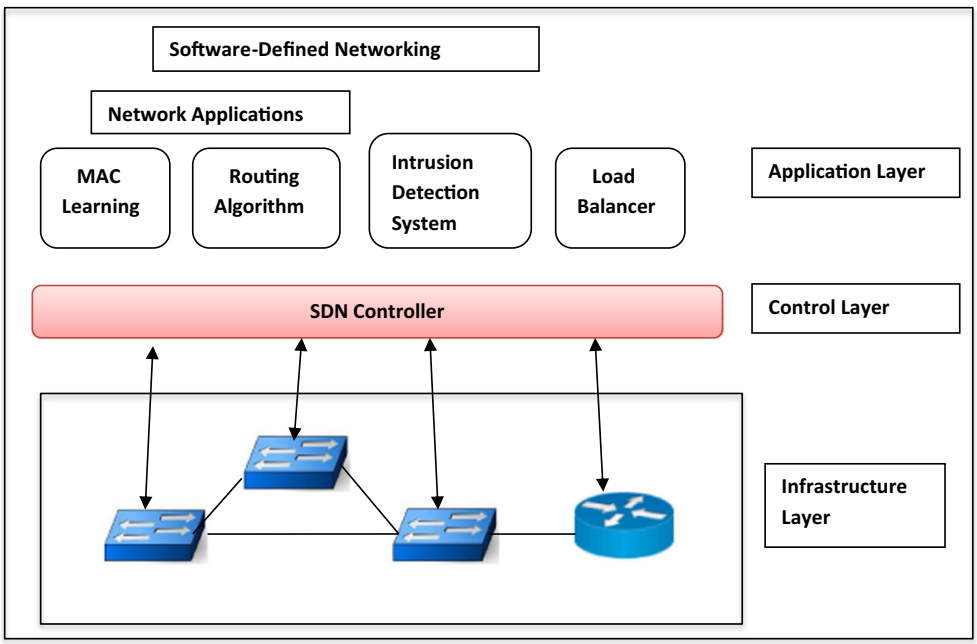

Fig. 3 SDN Architecture ([2])

mobile communication networks. SDN has the potential to fine tune mobile communication performance. The SDN architecture can be applied to wireless network environments such as wireless cellular communication, wireless mesh network, Wi-Fi access network and internet of things (IoT) etc. Leveraging SDN, IoT paradigm can also introduce scalability. Thus, by simplifying management and traffic engineering in wireless mesh networks and deploying crowd-sharing models, SDN creates opportunities for network connectivity and bandwidth sharing [36].

- **Data centers:** In a data center environment, optimal traffic engineering, network control, and policy implementations are required when operating at large scales. Using SDN based traffic orchestration, we can reduce network latency, and introduce security in an automated and dynamic fashion in the data centers [36].
- **SDN-Based Cloud:** Combining cloud techniques and SDN paradigm provides a close integration of applications in the cloud. With the network programmable interfaces and automation, SDN is a good tool to defeat cloud intrusion. Thus, SDN increases the service scalability in cloud environments [37].
- **Residential environment:** SDN framework allows users and service providers' greater visibility into residential and small office networks. SDN can implement anomaly detection systems in a SOHO network using programmability for greater accuracy and scalability [4].

3.2 SDN-based NIDS observation using ML/DL

SDN-based Intrusion detection system using ML/DL approach shows many advantages in terms of security enforcement, virtual management, and Quality of Service (QoS). SDN provides us a chance to strengthen our network security and provides flexibility to program network devices and eliminates hardware dependency. A brief overview and comparison of different solution for NIDS using SDN platform is shown in Table 2.

An SDN network with software switch implementations and programmable feature can be developed using simulation and emulation platforms. Open Flow is one of the most popular protocol standard [39, 40] that allows the implementation of the SDN concept in both hardware and software environments. There are other simulation tools, such as NS-2, Mininet [37], NS-*3*, OMNeT++ [38, 40, 41]. The vital part of an SDN networks the SDN controller, also known as a network operating system. SDN controller is responsible for concentrating communications with all programmable elements of the network, providing a combined view of the network. Currently, there are several SDN controllers such as NOX [42] and POX [43, 44]. Figure 4, an SDN-based NIDS architecture as depicted.

It can be observed that compare to ML, researchers started to apply deep learning techniques in the field of NIDS. Deep learning is capable of automatically finding a correlation in the data, so it is a prospective method for the next generation of intrusion detection techniques [10]. DL based approaches outperformed existing machine learning techniques when applied to various classification problems in SDN networks [8]. Most of the supervised ML algorithms are good at classification tasks, but not in modelling logic. DL based approaches outperformed existing machine learning techniques in logic modelling. As attacks are unknown, unsupervised learning algorithms such as stacked autoencoder, RNN and hybrid based algorithms will be the best for NIDS implementation in SDN platform.

In recent years, researchers are implementing ML based NIDS in SOHO networks using SDN environment and it was found that the IDS accuracy has greatly improved due to ML based algorithms and scalability of SDN.

Table 2 Comparison of SDN-based NIDS using DL approach

Publication	Method	Usage	Comparison
Syed Akbar Mehdi et al. [4]	Used four anomaly algorithms TRW-CB algorithm, rate limiting, maximum entropy detector and NETAD.	Anomaly Detection	Standardized programmability and can predict anomalies in SOHO Network
Rodrigo Braga et al. [38]	Used self-organizing maps an unsupervised artificial neural network.	Lightweight DDoS Flooding Attack	Efficient at detecting DDoS attacks but not have any flow rules installed.
Tuan A Tang et al. [6]	Used deep learning approached for flow-based anomaly detection	Anomaly Detection	Does not scale well commercial product or an alternative solution for signature-based IDS
Quamar Niyaz et al. [8]	Used stack auto-encoder, deep learning for feature reduction	DDoS Detection System	Can detect any DDoS attack, but has a Controller bottleneck in a vast network.
Damian Jankowski et al. [59]	Used self-organizing map and learning vector quantization.	Intrusion Detection	Can detect U2R attacks that include deep packet inspection technique.

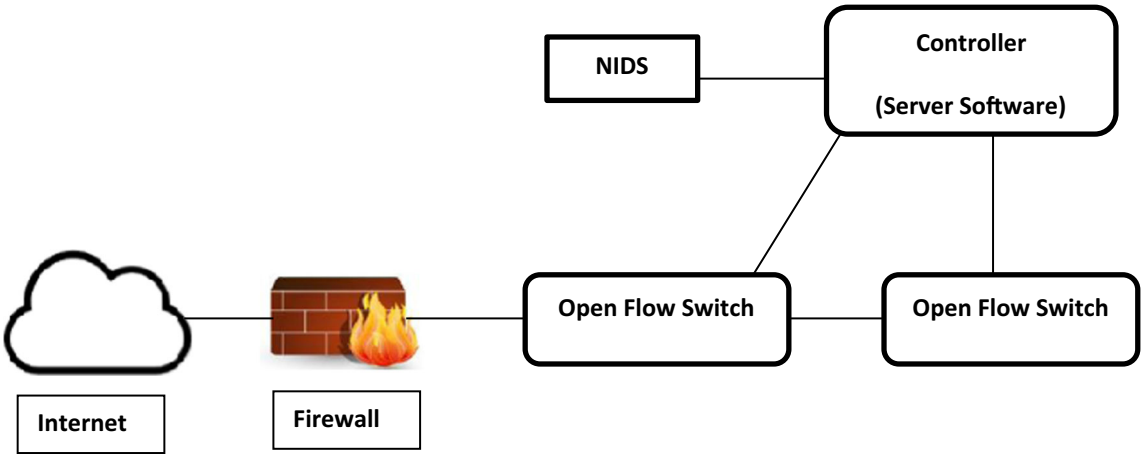

Fig. 4 Model of Intrusion detection system in SDN architecture (After [6])

4 Research challenges

There are some challenges while developing a flexible and efficient NIDS using ML/DL in SDN based networks [5].

- A predominant challenge is to choose appropriate feature-selection methods that can precisely determine the relevance of features to the intrusion detection task and the redundancy between these features [45]. Therefore, how to determine the optimum number of model parameters and how to improve the computational realism is a challenge in ML/DL [33].
- The existing intrusion detection dataset is not accurate for research predications for academic research as they require proper classification of data. Network researchers use synthetic data sets for network intrusion detection due to lack of better and more realistic datasets. It is essential to create datasets to ensure consistent and accurate evaluation of intrusion detection systems. For testing and evaluation of intrusion detection, several datasets are available. However, the most widely used evaluation datasets are the KDD Cup 1999 and its modified version, the NSL-KDD dataset for network-based intrusion detection systems [46].
- SDN-Based NIDS Challenges**, the fundamental challenge** of SDN-based NIDS is how to handle packet processing flows in an efficient way which is a big challenge to implement NIDS using ML/DL approach with high volume of data [47].
- SDN itself may be a target of various attacks such as DDoS. Forged traffic flows, vulnerabilities in switches, and attacks on the control plane are primary potential threat vectors in SDN. All these attacks can have a devastating impact on the overall network [48]. So, it is necessary to improve SDN security itself.
- With the application of SDN in larger networks, the network controllers could face a performance bottleneck due to a significant amount of incoming and forwarding data. Reduce controller bottleneck to implement NIDS is another research challenge [37].

In [49] authors compared Feature-Selection Methods for Intrusion Detection and they outlined the main disadvantages of various feature learning systems is their complexity and are expensive to implement. In recent years, there has been active research works on feature selection, where they use various feature selection methods such as principal feature analysis, Bi-Layer behavioural-based feature selection approach, and Random Forest to reduce feature [50–52]. In [53], support vector data description (SVDD) is used to automatically select the optimal feature combination for anomaly detection by applying feature selection techniques.

At present, the researchers are using some new data sets that are used around the world by universities, private industry and independent researchers. These databases are developed by research institutes like the University of New Brunswick ISCX 2012 Intrusion Detection, Evaluation Data Set [54], and the CIC DOS Dataset [55]. The ADFA-LD12 dataset is a worthy successor for the KDD dataset [56], and the UNSW-NB15 dataset [57] was also used for academic research purpose. WSN-DS [58] specialised dataset for wireless sensor network (WSN) is developed to detect and classify four types of denial of service (DoS) attacks in wireless sensor network.

5 Conclusion and future work

In this paper, we provided an overview of programmable networks and examined the emerging field of Software-Defined Networking (SDN). We also outlined various intrusion detections mechanisms using ML/DL approaches. We emphasized software-defined networking (SDN) technology as a platform using ML/DL approaches to detect vulnerabilities and monitor networks.

The use of deep learning has gained importance due to its efficiency in evaluating network security. Similarly, new methods of deep learning are increasing faster and efficient in data taxation. Various issues need to be considered while implementing NIDS, since the nature of the attacks are dynamic. So, adaptability of detection method is required. Developing a feature selection method with classifiers which reduces the dimensions of the dataset is an ongoing challenge. This is another field of research to classify proper dataset using DL techniques.

To design a centralized SDN controller, that can monitor and implement real-time intrusion detection in high-speed networks is a possible future direction and will be a challenging task. Most of the SDN-based NIDS architectures developed to identify mostly malicious activities in the SOHO network [39]. It is appropriate to note that none of the approaches implementing SDN-based NIDS are applied to critical infrastructure and high-speed network infrastructure. We think that with greater accuracy and scalability of SDN, the researchers can achieve ML/DL based NIDS on critical infrastructure.

We believe that this comprehensive survey could help R&D people to understand the development of NIDS in SDN context using DL approach.

References

1. Hewlett Packard Enterprise (2015) 2015 cost of cyber crime study: global, independently conducted by Ponemon institute LLC publication, Ponemon Institute research report. Avaiable https://www.accenture.com/t20170926T072837Z__w__/us-en/_acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf. Accessed 26 June 2017
2. Kreutz D, Ramos FMV, Verissimo PE, Rothenberg CE, Azodolmolky S (2015) Software-defines network- a comprehensive survey. Published in Proceedings of the IEEE, 103, 1
3. Aburomman AA, Reza MBI (2016) Survey of learning methods in intrusion detection systems. International conference on advances in electrical, electronic and system Engineering(ICAEES), Putrajaya, pp 362–365. https://doi.org/10.1109/ICAEES.2016.7888070
4. Mehdi SA, Khalid J, Khaiyam SA (2011) Revisiting traffic anomaly detection using software defined networking. In: Sommer R, Balzarotti D, Maier G (eds) Recent Advances in Intrusion Detection. RAID 2011. Lecture Notes in Computer Science, vol 6961. Springer, Berlin, Heidelberg
5. Garcı´a-Teodoroa P, Dı´az-Verdejo J, Macia´-Ferna'ndez G, Va´zquez E (2009) Anomaly-based network intrusion detection: Techniques, systems and challenges. J Comput Secur 28(1-2):18–28
6. Tuan TA, Mhamdi L, Mclernon D, Zaidi SAR, Ghogho M (2016) Deep learning approach for network intrusion detection in software defined networking. Int Conf Wirel Netw Mob Commun. https://doi.org/10.1109/WINCOM.2016.7777224
7. Open Networking Foundation (2013) SDN architecture overview, Version 1.0. Available https://www.opennetworking.org/images/stories/downloads/sdnresources/technical-reports/TR_SDN-ARCH-Overview-1.1-11112014.02.pdf. Accessed 27 June 2017
8. Niyaz Q, Sun W, Javaid AY (2016) A deep learning based DDoS detection system in software defined networking (SDN). CoRR abs/1611.07400. https://doi.org/10.4108/eai.28-12-2017.153515
9. Sezer S, Scott-Hayward S, Chouhan PK (2013) Are we ready for SDN? Implementation challenges for software-defined networks. In: IEEE Communication Magazine, vol. 51, no. 7, pp 36–43. https://doi.org/10.1109/MCOM.2013.6553676
10. Atkinson RC, Bellekens XJ, Hodo E, Hamilton A, Tachtatzis C (2017) Shallow and deep networks intrusion detection system: a taxonomy and survey. CoRR, arXiv preprint arXiv:1701.02145. 2017 Jan 9
11. Survey of Current Network Intrusion Detection Techniques https://www.cse.wustl.edu/~jain/cse571-07/ftp/ids/. Accessed 26 June 2017
12. Supervised and unsupervised machine learning algorithms http://machinelearningmastery.com/supervised-and-unsupervised-machine learning-algorithms/. Accessed 20 June 2017
13. Zamani M, Movahedi M (2015) Machine learning techniques for intrusion detection. CoRR, arXiv preprint arXiv:1312.2177. 2017 Jan 9
14. Thaseen S, Kumar Ch (2013) An analysis of supervised tree based classifiers for intrusion detection system. In: Proceedings of the international conference on pattern recognition, informatics and mobile engineering (P RIME). Pp. 21–22
15. Niyaz Q, Sun W, Javaid AY, Alam M (2016) A deep learning approach for network intrusion detection system. International conference wireless networks and mobile communications (WINCOM)
16. Zanero S, Savaresi SM (2004) Unsupervised learning techniques for an intrusion detection system. In: Proceedings of the ACM symposium on applied computing. Pages 412–419
17. Syarif I, Prugel-Bennett A, Wills G (2012) Unsupervised clustering approach for network anomaly detection. In: Benlamri R (eds) Networked Digital Technologies. NDT 2012. Communications in Computer and Information Science, vol 293. Springer, Berlin, Heidelberg
18. Tsai C, Hsu Y, Lin C, Lin W (2009) Intrusion detection by machine learning: a review. Expert Syst Appl 36:11994–12000
19. Bennett KP, Demiriz A (2017) Semi-supervised support vector machines. Neural Comput & Applic 28(5):969–978
20. Haweliya J, Nigam B (2014) Network intrusion detection using semi supervised support vector machine. Int J Comput Appl 85, 9
21. Chen C, Gong Y, Tian Y (2008) Semi-supervised learning methods for network intrusion detection. Int Conf Sys, Man Cybern, IEEE. https://doi.org/10.1109/ICSMC.2008.4811688
22. Deep learning stand to benefit to data analytics and HPC expertise http://www.cio.com/article/3180184/analytics/deep-learning-stands-to- benefit-from-data-analytics-and-high-performance-computing-hpc-expertise.html. Accessed 3 July 2017
23. LeCun Y, Bengio Y, Hinton G (2015) Deep learning review. Weekly journal of science in nature international. Nature 521, doi: https://doi.org/10.1038/nature14539
24. Convolutional Neural Networks (2017) http://eric-yuan.me/cnn/. Accessed 10 July 2017
25. Deng L, Yu D (2014) Deep learning methods and applications. Microsoft Research. Available https://www.microsoft.com/en-us/research/publication/deep-learning-methods-and-applications/. Accessed 10 July 2017
26. Alom MZ, Bontupalli VR, Taha TM (2015) Intrusion detection using deep belief networks. Aerospace and electronics conference, NAECON. IEEE
27. Tutorial http://ufldl.stanford.edu/tutorial/supervised/ConvolutionalNeuralNetwork/. Accessed June 15 2017
28. Vyas A (2017) Deep learning in natural language processing" in mphasis, deep learning- NL_whitepaper

29. Hughes T, Mierle K (2013) Recurrent neural networks for voice activity detection IEEE International Conference on Acoustics, Speech and Signal Processing, Vancouver, BC, pp 7378–7382. https://doi.org/10.1109/ICASSP.2013.6639096
30. Salama MA, Eid HF, Ramadan RA, Darwish A, Hassanien AE (2011) Hybrid intelligent intrusion detection scheme. Soft computing in industrial applications in advances in intelligent and soft computing book series (AINSC, volume 96), pp 293–303
31. Fiore U, Palmieri F, Castiglione A, Santis AD (2013) Network anomaly detection with the restricted Boltzmann machine. Neurocomputing 122(25):13–23
32. Eid HFA, Darwish A, Hassanien AE, Abraham A (2010) Principal components analysis and support vector machine based intrusion detection system. International conference intelligent systems design and applications (ISDA)
33. Wang L, Jones R (2017) Big data analytics for network intrusion detection: a survey. Int J Netw Commun. https://doi.org/10.5923/j.ijnc.20170701.03
34. Open Networking Foundation (2014) SDN architecture, Issue 1 June 2014 ONF TR-502
35. Nunes BAA, Mendonca M, Nguyen XN, Obraczka K and Turletti T (2014) 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. https://doi.org/10.1109/SURV.2014.012214.00180
36. Bakshi T (2017) State of the art and recent research advances in software defined networking. In Wireless Communications and Mobile Computing, 2017, 1530-8669, Hindawi Publishing Corporation
37. Yan Q, Yu FR, Gong Q and Li J (2016) Software-defined networking (SDN) and distributed denial of service (DDoS) attacks in cloud computing environments: A survey, some research issues, and challenges. IEEE Communications Surveys & Tutorials, vol. 18, no. 1, pp 602–622 Firstquarter 2016. https://doi.org/10.1109/COMST.2015.2487361
38. Braga R, Mota E, Passito A (2010) Lightweight DDoS flooding attack detection using NOX/OpenFlow. 35th Annual IEEE conference on local computer networks, Denver, Colorado
39. Open Networking Foundation, Jun (2014) [Online]. Available: https://www.opennetworking.org/. Accessed 10 July 2017
40. Prete LR, Shinoda AA, Schweitzer CM, De Oliveira RLS (2014) Simulation in an SDN network scenario using the POX controller. 2014 I.E. Colombian Conference on Communications and Computing (COLCOM), Bogota, pp 1–6. https://doi.org/10.1109/ColComCon.2014.6860403
41. Open Flow [Online]. Available: http://www.openflow.org/. Accessed 12 July 2017
42. NOX. [Online]. Available: http://www.noxrepo.org/nox/about-nox/. Accessed 12 July 2017
43. POX. [Online]. Available: http://www.noxrepo.org/pox/about-pox. Accessed 12 July 2017
44. Kaur S, Singh J, Ghumman NS (2014) Network programmability using POX controller. International conference on communication, computing & systems, at SBS Staten technical campus, Ferozepur, Punjab, India, volume: 1
45. Nguyen HT, Petrovic S, Franke K (2010) A comparison of feature-selection methods for intrusion detection. In: Kotenko I, Skormin V (eds) Computer Network Security. MMM-ACNS 2010. Lecture Notes in Computer Science, vol 6258. Springer, Berlin, Heidelberg, pp 242–255
46. Gogoil P, Bhuyan MH (2012) Packet and flow-based network intrusion dataset. International conference on contemporary computing IC3, pp 322–334
47. Hu F, Hao Q, Bao K (2014) A survey on software-defined network and openFlow: from concept to implementation. IEEE communication surveys & tutorial 16:4
48. Alom MZ, Bontupall VR, Taha TM (2015) Intrusion detection using deep belief networks. In: Aerospace and electronics conference, NAECON
49. Coates A, Lee H, Ng Andrew Y (2011) An analysis of single-layer networks in unsupervised feature learning. In: Proceedings of the fourteenth international conference on artificial intelligence and statistics, PMLR 15:215–223
50. Lu Y, Cohen I, Zhou XS, Tian Q (2014) Feature selection using principal feature analysis. Pattern Recogn Lett 49:33–39
51. Eid HF, Salama MA, Hassanien AE, Kim TH (2011) Bi-layer behavioral based feature selection approach for network intrusion classification. Commun Comput Inf Sci Book Ser 259:195–203
52. Hasan MAM, Nasser M, Ahmad S, Molla KH (2016) Feature selection for intrusion detection using random forest. In: Journal of information security, pp 129–140
53. Kloft M, Brefeld U, Dussel P, Gehl C, Laskov P (2008) Automatic feature selection for anomaly detection. In: Proceedings of the 1st ACM workshop on AISec, Pages 71–76, Alexandria, Virginia, ACM New York, USA
54. Shiravi A, Shiravi H, Tavallaee M, Ghorbani AA (2012) Toward developing a systematic approach to generate benchmark datasets for intrusion detection. Comput Secur 31(3):357–374
55. University of New Brunswick (2017) [Online] available http://www.unb.ca/cic/research/datasets/dos-dataset.html. Accesses 22 June 2017
56. Creech G, Hu J (2013) Generation of a new IDS test dataset: time to retire the KDD collection. Wirel Commun Netw Conf (WCNC). https://doi.org/10.1109/WCNC.2013.6555301
57. Nour M, Slay J (2016) The evaluation of network anomaly detection systems: statistical analysis of the UNSW-NB15 data set and the comparison with the KDD99 data set. Inf Secur J: A Glob Perspec, pp 1–14
58. Almomani I, Al-Kasasbeh B, Al-Akhras M (2016) WSN-DS: a dataset for intrusion detection systems in wireless sensor networks. J Sens 16p
59. Jankowski D, Amanowwicz M (2016) On efficiency of selected machine learning algorithms for intrusion detection in software defined networks. Int J Electron Telecommun, 62(3):247–252