State of the art literature review on Network Anomaly Detection with Deep Learning

Tero Bodström and Timo Hämäläinen

Faculty of Information Technology, University of Jyväskylä,
P.O. Box 35, (Agora), 40014 Jyväskylä, Finland
{tero.bodstrom@gmail.com,timo.hamalainen@jyu.fi}

Abstract. As network attacks are evolving along with extreme growth in the amount of data that is present in networks, there is a significant need for faster and more effective anomaly detection methods. Even though current systems perform well when identifying known attacks, previously unknown attacks are still difficult to identify under occurrence. To emphasize, attacks that might have more than one ongoing attack vectors in one network at the same time, or also known as APT (Advanced Persistent Threat) attack, may be hardly notable since it masquerades itself as legitimate traffic. Furthermore, with the help of hiding functionality, this type of attack can even hide in a network for years. Additionally, the expected number of connected devices as well as the fast-paced development caused by the Internet of Things, raises huge risks in cyber security that must be dealt with accordingly. When considering all above-mentioned reasons, there is no doubt that there is plenty of room for more advanced methods in network anomaly detection hence Deep Learning based techniques have been proposed recently in detecting anomalies.

Keywords: Network attacks, Anomaly detection, Deep learning

1 Introduction

The purpose of this study is to highlight major challenges in network anomaly detecion with deep learning by focusing on recent research in the field. Among the growing number of data and network connected devices, the challenge is different attack types such as APT, DDoS and Zero-day. They each have a unique behavioural pattern and the difficulty is to come up with a solution that has the capability to detect all of them efficiently in modern networks. In this study following aspects are considered: intended attack type detection, functional differences as well as the differences in detection accuracy.

By definition, anomalies are observations which differ from other observations enough to arise suspicion. Suspicious observations in network traffic can be caused by either legitimate events or non legitimate events and the purpose of

anomaly detection is to divide normal and anomalous data with different techniques[3, 4]. However, any suspicious event has to be treated as hostile, until it is verified and proved to be non-hostile.

Most of the presented studies in this paper are focused on DDoS, Zero-day and web attacks. There is less current research material on APT attacks for some unknown reason and one focus in this paper is to evaluate the possibility for using Deep Learning to detect APT attacks.

This paper unfolds as follows: in the second section research papers based on different anomaly detection technologies where deep learning methods were used to detect anomalies is discussed. The third section summarizes perceived improvements for the presented researches. The fourth section concludes this review discussing advantages and disadvantages of selected research presented along the paper.

2 Network Anomaly Detection With Deep Learning

In this section different methods that use deep learning for network anomaly detection are presented. These methods focus on one or more simultaneous attack types.

Chuanlong Yin et al. proposed a deep learning based intrusion detection (RNN-IDS) method in their paper. The purpose of the study was to improve intrusion detection systems with recurrent neural networks, system performance and review the possibility to solve two types of classification problems: i) binary and ii) multiclass classification. These classification problems were chosen since first, the data must be classified as anomalous or legitimate and then categorized for different attack types. Instead of more traditional machine learning methods, such as support vector machine(SVM), K-Nearest Neighbour (KNN), random forest(RF) and so on, the authors selected a recurrent neural network deep learning method as it surpasses traditional methods due to the ability of processing high-dimensional data. The proposed classification methods were tested with binary and multiclass classification with five categories as follows: i) normal, ii) DoS, iii) User to Root (U2R), iv) Probe (Probing) and v) Root to Local (R2L).[1]

The authors used Python written Theano as a deep learning framework and selected RNN to be used because of high amount of dimensions in the data. They selected NSL-KDD dataset to be used during tests, as it resolves KDDCup99 dataset known problems, such as inherent redundant records[1, 5–7]. NSL-KDD dataset includes 41 variables, of which 38 are numeric and 3 non-numeric. For training RNN and executing detection tests, they preprocessed the data which lead to an increase in the number of dimensions, from 41 to 122. This happens when a variable has multiple possible values and every value has to be presented as unique in a numeric matrix with zeros and ones.[1]

As mentioned earlier, the authors executed comparison tests for both, binary and multiclass classification. They tested different hidden node numbers and

learning rates for optimizing accuracy rate. For binary classification it was found that with 100 epochs, 80 hidden nodes and 0.1 learning rate the best accuracy was achieved. With multiclass classification it was found that 80 epochs, 80 hidden nodes as well and 0.5 learning rate presented the highest accuracy. Test results showed that RNN has higher accuracy and lower false positive rate than compared traditional machine learning methods.[1]

For the future work C. Yin et al. will put focus on GPU acceleration to reduce training time and how to avoid exploding and vanishing gradients. Besides those, they will study how to improve classification performance of LSTM and Bidirectional RNNs algorithms for the intrusion detection purposes.[1]

The implementation of basic RNN that the authors proposed handled 122 dimensional data with respectful results, thus outrunning traditional ML methods. Multidimensional handling is extremely important when detecting APT attacks since the difference to normal data can be almost non-existent, possibly only some bits at binary level.

Xiaoyong Yuan et al. proposed Bidirectional Recurrent Neural Network based DDoS detection in their paper. The purpose was to improve DDoS detection rate, as traditional machine learning methods are limited by small depth of representation models. They stated that DDoS attack traffic is hard to detect automatically since the traffic is very similar to normal traffic and attackers try to mimic normal high usage peaks by using Flash-crowd method. In addition, statistical based detection performs well with specific DDoS and needs preprossessing metrics for different attacks. They proposed a model called *DeepDefence* which they tested with the following deep learning methods for the model: i) Recurrent Neural Network (RNN), ii) Long Short-Term Memory Neural Network (LSTM) and iii) Gated Recurrent Unit Neural Network (GRU), and executed comparison tests with more traditional Random Forest ML method.[2]

In the prosed method, the authors designed Bidirectional Recurrent Neural Network, where input nodes has two separated parallel hidden layers: i) Forward and ii) Backward recurrent layer. Data passes through both hidden layer sets and results are connected in a latter layer before the prediction of an anomaly. RNN was selected as it handles historical information problem well (especially LTSM and GRU), that is, the method improves performance based on historical data patterns, whereas single-packet detection cannot perform.[2]

For testing the proposed method, seven day recording of ISCX2012 dataset was selected and extracted to two separate datasets, *data14* and *data15*. First they tested different RNN methods with both datasets and compared each other to find the best performing method. All RNN's performed with high accuracy rate, but eventually LSTM showed highest accuracy rate with *data14* (97.996%) and 3LTSM with *data15* (98.410%). Secondly they tested random forest accuracy rate with same datasets. Tests showed lower accuracy rate, but also a slight gap between datasets: 97.117% accuracy with *data14* and 92.518% with *data15*.[2]

X. Yuan et al. stated that for the future work they are increasing the variety of DDoS vectors and system settings in order to execute performance tests in

different environments to verify robustness. They will build *Deep DDoS Defense system* based on proposed method and execute tests in real environments.[2]

The proposed RNN showed interesting results. The accuracy rates were almost equal with 0.099% difference while with random forest the difference was 4.599%. Based on the results recurrent neural networks perform in a more stable manner than traditional machine learning methods. LTSM is also worthy for further study in APT attack detection as it can recall historical information which may be crucial when detecting APT attacks.

Sergey Andropov et al. proposed multilayer perceptron Artificial Neural Network (ANN) with backspace propagation algorithm training in their paper. The purpose was to research the possibility to detect attacks that are unknown which is difficult if not even impossible with signature based detection methods[3, 7]. Anomalies can be caused by network attacks, malware and hardware or software malfunctions, and any kind of anomaly should be treated as dangerous. Changes in network topology, such as new network device or software gets installed or new end-user device with previously unknown software is added, occurs from time to time and causes new patterns or behaviour in network. However, neural networks permit these changes and is able to adapt by adjusting its weights accordingly.[3]

The proposed method has two functional states: i) offline and ii) online traffic analysis and it uses data aggregation to detect patterns in the elseways highly variable traffic data. The authors implemented Netflow protocol to gather information from network devices, which was then filtered and aggregated for anomaly detection process in ANN. Aggregation was executed with different criteria, for example: i) number of packets per hour, ii) average packet size and iii) port usage, which were used as an input to neural network. They used three layer ANN: i) input layer, ii) hidden layer and iii) output layer, where output layer has a neuron for every anomaly the method is able to detect and two extra neurons, one for normal and one for unknown. They selected six input neurons, 10 neurons in a hidden layer and seven output neurons, and used Sigmoid function for classification in both hidden and output layer.[3]

For testing the proposed methods, a local ISP collected data for the authors from several hundred L2 nodes for a period of one month and this dataset was considered as a normal traffic. Authors created several small-scale anomalies for testing purposes, such as: i) DoS and DDoS attacks, ii) port scans, iii) email spamming and iv) routers turning off. They also created a custom anomaly to test if the neural network can detect an unknown anomaly class. These created anomalies were injected into normal traffic dataset before executing detection tests. The proposed ANN was able to detect both, known and unknown anomalies with high accuracy, however test results show that idle scan is the most difficult to detect. Custom anomaly had the lowest accuracy with 150000 classification iterations, ARP spoofing the second lowest and idle scan third lowest. After 300000 classification iterations all other anomalies had over 80% accuracy, while idle scan stayed below 80%.[3]

S. Andropov et al. mentioned briefly that for the future work their focus is in "*reducing the false positive rates and optimizing the aggregation algorithms*".[3]

The proposed multi-output layer method gives more detailed information about the anomaly than the boolean alternative due to classification. This type of method can be useful in detecting APT attacks since it has multiple simultaneous attack vectors. It would be interesting to see how the idle scan detection accuracy could be increased, for example by optimizing the ANN, perhaps choosing different amount of hidden layers and neurons in a layer.

R. Can Aygun et al. proposed a deep learning based IDS for zero-day attack detection. The purpose was to improve zero-day attack detection with enhanced Autoencoder (AE) based models. Current IDS's are based on signature database from previous attacks and does not detect well unknown new attacks even if the database is kept up to date. They stated that, because of IDSs lack of ability to detect earlier unknown attacks, the research community is moving towards the machine learning based smart IDS, which can adopt new and constantly changing network attacks and reduces the existing problem from occurring.[4–7]

The authors proposed AE with stochastic anomaly threshold determination algorithm. They tested and compared performance of stochastic and deterministic AE's with the proposed algorithm. AE has two basic functionalities, i) encoding and ii) decoding, whereas the number of nodes in input layer and output layer remain the same. The method uses encoding for trying to express input with smaller amount of units in a hidden layer and then reconstructs the encoded input in decoding phase as an output. However, AE's known problem is that it can become as an identity function due to training data and therefore may perform with low accuracy. To avoid that problem, the authors selected stochastic de-noising method. A semi supervised training method was used for training AE because of more satisfactory detection accuracy for zero-day attacks. They only used normal traffic data for the training process and afterwords the model was used for classifying instance. The data that was not recognized as normal traffic was labelled as anomalous. However, the detection results must be interpreted correctly with proper thresholds since the semi supervised training has a known problem called reconstruction error which will be high for anomalous and low for normal data.[4]

NSL-KDD dataset was selected for testing the proposed smart IDS. The dataset includes different datasets for training and testing purposes, the test set also has completely different attack types than the training set and is therefore well suited for zero-day detection tests. The data was pre-processed and feature number increased from 41 to 121 and then dataset was scaled to range of [0,1]. Evaluation test results showed that the deterministic detection method performed with 88.28% and the stochastic method with 88.65% accuracy respectfully.[4]

The proposed method performed with decent detection rate for detecting zero-day attacks and therefore could be studied also for APT detection. How-

ever, automated interpretation for detection results is recommended.

Nguyen T. Van et al. proposed deep learning based Network Intrusion Detection System (NIDS) in their paper. The purpose was to implement DL method to NIDS to gain anomaly-based detection and to be able to detect known and unknown attacks[5]. Nowadays enterprise networks have a significant importance and the growing number of devices and vulnerabilities has lead to a situation were security solutions have to be more flexible to adapt to constantly changing environment variables, and deep learning methods are well suited to[4–7]. The authors stated that anomalies can be categorised in three ways: i) point anomaly, ii) contextual anomaly and iii) collective anomaly, and these relate closely to network attacks such as Denial of Service (DOS), Probe, User to Root (U2R) and Remote to local (R2L). NIDS must have the ability to detect both known and unknown anomalies as well as to analyse and classify all attack types.[5]

Intrusion traffic differs from normal and hence anomaly detection methods are suitable for intrusion detection, and the authors proposed a method where they used deep learning self-learning competence in an effective way. They used stacked method for constructing multi-layer neural networks. That is, they used three combined neural networks, where the output from the first neural network's hidden layer was used as an input data to the second neural network and finally the detection and classification was done based on the output from the third neural network. Restricted Boltzmann Machines (RBM) and Autoencoder (AE) were selected for neural network pre-training.[5]

For detection tests, they selected KDDCup99 dataset and executed tests with both selected methods. Even though the authors stated that the widely used KDDCup99 dataset is not realistic since it is obsolete and lacks of modern network features, it was used in their tests[1, 5–7]. Test results showed that both methods have high detection accuracy, but AE performs better than RBM when classifying data into normal and four different attack types. However AE has longer execution and pre-training time.[5]

For future work N. T. Van et al. mentioned two things, first they will study how to implement system to parallel platforms for gaining more computational speed. Secondly they want restudy pre-training techniques to optimize and reduce oscillation in order to decrease training errors and increase detection accuracy.[5]

Stacked neural network is an interesting idea and could be studied for APT detection. However, more relevant datasets should be used for modern detection system testing to verify if the test results get affected.

Sunhee Baek et al. proposed Unsupervised Labeling for Supervised Anomaly Detection, that is, combination of functionality from both, supervised and unsupervised training methods to improve detection accuracy. This combined method was studied due to problems of individual trainings methods which they addressed as follows: i) Supervised learning method uses labelled data which has high accuracy and it executes fast data point tests, however the downside is

that all possible data is not available and thus cannot be labelled as detection expects, ii) Instead of labelling, unsupervised learning method does data classification during the learning process and requires less data for detection, however it has low detection accuracy and high runtime complexity[6]. The purpose was to improve anomaly detection in an enterprise and ISP networks, where fast detection is critical for business.[4–6]

In the proposed method, the authors were more interested in detecting anomalies than classifying attack types. By preliminary research they defined traditional anomaly detection as follows: "*Assumption: Normal data instances belong to large and dense clusters, while anomalies either belong to small or sparse clusters*"[6]. Based on the mentioned phrase, parameters were defined for size *(size := {small or not})* and density *(density := {sparse or not})*, and by defining this way mathematical definitions were created. The authors rephrased earlier assumptions for anomaly detection by proposing the following method: i) extremely dense cluster is labelled as anomalous, ii) small or sparse cluster is labelled as anomalous and iii) otherwise cluster is labelled as normal. The authors redefined the mathematical format of clustering, based on their new definition, so that it suited the proposed method. They tested and optimized the method and finally labelled testing data with it. The authors then selected four supervised known and widely used methods: i) Naive Bayes, ii) Adaboosting, iii) SVM and iv) Random Forest and trained and tested all with the labelled data.[6]

For testing purposes NSL-KDD dataset was selected due the know problems in KDDCup99 dataset[1, 5–7]. First they tested performance of earlier mentioned traditional anomaly detection, which overall detected anomalies poorly. Tests were executed with five different cluster size (16, 32, 64, 128 and 256) and highest performance was found with cluster size 16, only 62% accuracy. However, the accuracy improved from 62% to 88% with the authors proposed rephrased method using the same cluster size 16. Finally they tested four supervised methods with labelled data and different cluster sizes. Even though the cluster size and dataset varied the test results showed that, by training supervised method with earlier labelled data by unsupervised method, the anomaly detection performs with high accuracy.[6]

S. Baek et al. mentioned that for future work they will develop a method for minimizing randomness of K-Means clustering. They were thinking that one possible method could be to including results of multiple runs for gaining more coherent results, with the help of quorum method. Another possibility would be reducing data dimensions to gain improvement for classification.[6]

Test results showed that by combining highly performing functionality from different methods, it is possible to improve overall performance. On the other hand, it would be interesting to see what is the performance accuracy for classifying different attack types with the proposed method. As in some cases only detecting anomalies does not fulfill the priorities of incident response - attack type classification is required so that most urgent and dangerous attacks can be attended and dealt with at first.

Vrizlynn L. L. Thing proposed Network Anomaly Detection and Attack Classification method for IEEE 802.11 standard wireless networks. The purpose was to classify different type of attacks in wireless networks with deep learning. Besides legitimate traffic, attacks were classified for three types: i) flooding, ii) injection and iii) impersonation type attacks. Wireless network anomaly detection was selected due to growing number of smart home, smart city and IoT solutions and devices, as their communication largely depends on wireless networks and IEEE 802.11 is de-facto standard. Wi-Fi protocol has various vulnerabilities and it has been intensively surrounded by attacks. This causes high level risks to end users and enterprises, including espionage and identity, credit card and money theft. According to authors, it is not enough to treat anomalies as a binary problem but classification is also needed for later analysis and possible recovery operations[7], including software vulnerability patching.

Stacked Auto-encoder (SAE) neural network was selected for implementing the proposed method. The authors proposed two SAE frameworks, with two and three hidden layer neural networks. In both frameworks, 256 neurons in the first and 128 in the second hidden layer were used. In addition, the latter framework had 64 neurons in the third layer. For the activation function selection they executed a test with following functions: i) Sigmoid function, ii) Rectified Linear Unit (ReLU), iii) Leaky ReLU (LReLU) and iv) Parametric Rectified Linear Unit (PReLU). After the activation function, the method executed Softmax regression for prediction, as it supports multi-class classification, while logistic regression supports only binary classification.[7]

For testing purposes the authors created the dataset to be used, as they could not use raw TCP dumps due to the different approach. They created a lab environment (WEP encrypted access point (AP)) with desktop machine, two laptops, two smart phones, a tablet and a smart TV to generate wireless legitimate traffic and capture it directly from the air. Kali Linux was used to execute 15 type of attacks and in addition several penetration testing tools were used. They classified and defined attacks as follows: i) injection, high number of correctly encrypted data frames, ii) flooding, high volume of management frames per unit time and iii) impersonation, introduce an access point to broadcast beacon frames to advertise a pre-existing network(victims network). Tests were executed with two SAE frameworks and all four action functions with the created data set, including 15 attack types, where seven were previously unknown. Results showed that two hidden layer framework with PReLU action function had highest prediction overall accuracy, respectful 98.6688%, and it was able to detect all categories with high and balanced manner. Based on test results, they were able to determine that impersonation attacks are most challenging to detect, but proposed method improved accuracy significantly compared to earlier studies.[7]

The proposed method used standard protocol traffic for anomaly detection instead of raw TCP dump. It would be worth studying if this type of approach can be addressed with wireless protocols such as Bluetooth, LoRaWan, ZigBee and others used in sensor networks employed in IoT-systems. The research results

showed also that it is truly important to optimize neural networks as varying the amount of hidden layers and different activation functions can give significantly different predictions with the same dataset.

Wei Wang et al. proposed malware traffic classification with Convolutional Neural Network (CNN) by transforming traffic data to images. This selected and proposed method does not require any hand-designed features but instead it takes raw data as an input and classifies the raw data by transforming it to images. The author claims, this was the first attempt to use representation of raw data to classify malware traffic.[8]

Classifying traffic, the authors used traffic granularity and packet layers, which enabled OSI or TCP/IP layer selection for each packet. In their proposed method, traffic granularity included: i) TCP connection, ii) flow, iii) session, iv) service, and v) host and besides those, they used flow and session information. Flow packets were defined as follows: i) source IP, ii) source port, iii) destination IP, iv) destination port and v) transport-level protocol, while sessions were defined as bidirectional flows. Four types of data representations were defined to reduce image size and eliminate session problems with IP and MAC addresses. The defined presentations were: Flow + All, Flow + L7, Session + All, Session + L7 (L7 is OSI layer 7).[8]

For testing purposes the authors created USTC-TFC2016 dataset and developed data-preprocessing toolkit USTC-TK2016. They mentioned that KDD-Cup99 and NSL-KDD offers multiple features but did not meet the requirements for raw data detection. The specific dataset was created by collecting data from multiple sources, ten different sets of malware traffic data from public websites and normal traffic was collected with IXIA BreakingPoint simulator and included ten common office software traffic datasets. They executed tests with two separate datasets for all four representations, that is eight tests in total. The test data was preprocessed with following steps: i) traffic split, ii) traffic clear, iii) image generation and iv) IDX conversion, that is, conversion from raw traffic data to CNN input data. They selected a static image size, 784 bytes, and for smaller image sizes they added 0x00 padding to achieve the correct size and larger image sizes were trimmed down to correct size. With the toolkit they developed they generated 752,040 records for testing purposes. The authors took also visual test for images and mentioned that different classes had "*obvious discrimination degree and each class of traffic has high consistency*"[8]. Comparison test results showed that *Session + All* representation had highest accuracy and average accuracy was respectful 99.41%.[8]

W. Wang et al. briefly stated that for the future work they are planning to improve the proposed method's capability for malware traffic data detection and identification.[8]

An interesting different approach for anomaly detection with extremely high accuracy. One thing that paper did not mention though is what is the processing time for raw data to CNN input data, that is, real time detection performance. In case the transformation is time-consuming, the proposed method is not suitable

for real time detection. The raw data approach could be used for APT detection without the traffic clear process.

Youbiao He et al. proposed a real-time False data injection (FDI) detection from Smart Grids with deep learning. Smart power grid monitoring and communications are moving towards IP networks to gain quality and intelligent functionalities. This progress also increases the possibility to FDI attacks, and the main focus was to improve detecting electricity thefts executed by FDI. Smart power grids are complex interconnected systems including Phasor Measurement Units (PMUs), smart meter, Remote Terminal Units (RTUs) and Supervisory Control and Data Acquisition (SCADA) system, where the latter is the main target for FDI attacks. System state information is vital for stability and efficiency of power grids, which is commonly part of the state level critical infrastructure.[9]

The authors proposed an extended Deep Belief Network (DBN) for anomaly detection, that is, "*Conditional Deep Belief Network (CDBN), that exploits Conditional Gaussian-Bernoulli RBM (CGBRBM) to extract high-dimensional temporal features*"[9]. The proposed CDBN method differs from earlier studied CDBNs by functions: while earlier has been studied with time-series model, the authors designed a method to act as a classifier. Other differences were, that the proposed method carried out CGBRBM only in the first hidden layer and Restricted Boltzmann Machine (RBM) for the rest of the hidden layers. Different methods for hidden layers were selected to reduce training and execution time complexity. System performance depends heavily on sensitivity of the pattern detections, difference in patterns of normal data and FDI compromise data. The proposed method leans heavily to static physical topology of power system.[9]

For testing purposes the authors trained CGBRBM and RBMs using unsupervised methods and final binary prediction was executed with Sigmoid activation, which indicated normal or compromised data. They collected data from real world sources to test simulation purposes, which contains small amount of compromised data and they generated artificially labelled compromised data with similar patterns as gathered real world compromised data had. Instead of TCP dump or raw data, the authors used IEEE 118-bus and IEEE 300-bus systems and their specific load profile data, that is used for tracking user power consumption. The proposed system was tested against various methods such as Artificial Neural Network (ANN) and Support Vector Machine (SVM) to compare their detection and scalability performances. Test results showed that the proposed method overall had higher detection accuracy with extremely low false positive and false negative rate.[9]

For the future work Y. He et al. mentioned two separate things, first they will expand research for modelling FDI attacks behaviour more practical way. Secondly, they will study what is the minimum number of required sensing units for their proposed method to still perform detection efficiently.[9]

The authors research shows how versatile deep learning is for anomaly detection, it can be applied to multiple systems where data is processed. Moreover, it would be interesting to see what kind of changes the proposed method requires

to make it more flexible and adaptive to changing power system topologies.

3 Summary of further improvements

In this section the perceived improvements for more precise anomaly detection is presented. These identified concerns vary from single to multiple papers.

Even though numerous papers mentioned that KDDCup99 is not realistic, data is obsolete and lack of modern network traffic, it is widely used for benchmarking new methods. The research community should go forward and look for present day datasets or create those to substitute KDDCup99, as in some papers researchers had already done.

In some of the papers only certain parts of IP and TCP headers were selected for the anomaly detection, such as source and destination IP's and ports. These types of solutions can limit the detection capability due to the vast amount of the possibly useful missing data.

Several research showed that Neural Networks have higher detection rate for the earlier unknown attacks. Due to the computational complexity and the hardware requirements, NN's have a negative impact for the detection systems cost structure. In a high velocity data centre hardware prices can increase significantly, in order to gain sufficient detection speed.

Another concern while using NN's is required amount of the training data. The detection rate highly depends on the amount of training data and cannot perform with a low detection rate without the sufficient amount of it.

Some of the papers focused on binary classification, normal traffic or anomalous. This type of solution do not give enough information of the actual attack vector, which can be crucial for incident investigations. Another important point with the binary classification is the false alarm rate, the false negative to be more precise. The false negative rate has to be extremely low or otherwise data will be incorrectly classified as a normal traffic.

4 Conclusion

The papers reviewed showed that different Deep Learning methods vary in their performance to detect anomalies. Every method had its advantages and disadvantages, but most of these methods detect previously unknown attacks extremely well. However, neural networks has a downside, they require more computational power that can cause also problems in real-time detection in high velocity networks, if hardware is not powerful enough. Another disadvantage is that it requires more training data to gain sufficient accuracy. On the other hand, neural networks capability to adapt to rapidly changing network environments by self learning, to handle multi-dimensional data and to detect previously unknown attacks gives a huge advantage for detecting sophisticated attacks such as

APT since it tries to act undetected as long as possible and mimic normal traffic. They are known to be hiding in networks even for years and neural networks are well suited for detecting those by reducing detection time, as they are difficult to detect in a real-time anyway.

When developing Deep Learning anomaly detection systems and methods, these advantages and disadvantages should be further considered, as they can help to define what could be the actual focus of the work. With current practices a system or a method that could detect all types of attacks, not to mention in a real-time environment, requires enormous resources and might be still even impossible to implement.

References

1. Yin, C., Zhu, Y., Fei, J., He, X.: A Deep Learning Approach for Intrusion Detection Using Recurrent Neural Networks. IEEE Access, pp. 21954 - 21961 (2017). https://doi.org/10.1109/ACCESS.2017.2762418
2. Yuan, X., Li, C., Li, X.: DeepDefense: Identifying DDoS Attack via Deep Learning. 2017 IEEE International Conference on Smart Computing (SMARTCOMP) (2017). https://doi.org/10.1109/SMARTCOMP.2017.7946998
3. Andropov, S., Guirik, A., Budko, M., Budko, M.: Network Anomaly Detection using Artificial Neural Networks. In: 2017 20th Conference of Open Innovations Association (FRUCT) (2017). https://doi.org/10.23919/FRUCT.2017.8071288
4. Aygun, R.C., Yavuz, A.G.: Network Anomaly Detection with Stochastically Improved Autoencoder Based Models. In: 2017 IEEE 4th International Conference on Cyber Security and Cloud Computing, pp. 193-198 (2017). https://doi.org/10.1109/CSCloud.2017.39
5. Van, N., Thinh, T., Sach, L.: An anomaly-based Network Intrusion Detection System using Deep learning. In: 2017 International Conference on System Science and Engineering (ICSSE), pp. 210-214. https://doi.org/10.1109/ICSSE.2017.8030867
6. Baek, S., Kwon, D., Kim, J., Suh, S.C., Kim, H., Kim, I.: Unsupervised Labeling for Supervised Anomaly Detection in Enterprise and Cloud Networks. In: 2017 IEEE 4th International Conference on Cyber Security and Cloud Computing, pp. 205-210. https://doi.org/10.1109/CSCloud.2017.26
7. Thing, V.L.L., IEEE 802.11 Network Anomaly Detection and Attack Classification: A Deep Learning Approach. In: 2017 IEEE Wireless Communications and Networking Conference (WCNC) (2017). https://doi.org/10.1109/WCNC.2017.7925567
8. Wang, W., Zhu, M., Zeng, X., Ye, X., Sheng, Y.: Malware Traffic Classification Using Convolutional Neural Network for Representation Learning. In: 2017 International Conference on Information Networking (ICOIN), pp. 712-717 (2017). https://doi.org/10.1109/ICOIN.2017.7899588
9. He, Y., Mendis, G.J., Wei, J.: Real-Time Detection of False Data Injection Attacks in Smart Grid: A Deep Learning-Based Intelligent Mechanism. IEEE Transactions on Smart Grid, pp. 2505-2516 (2017). https://doi.org/10.1109/TSG.2017.2703842