Developing a Siamese Network for Intrusion Detection Systems

Hanan Hindy
Christos Tachtatzis
Robert Atkinson
Ethan Bayne
Xavier Bellekens

http://dx.doi.org/10.1145/3437984.3458842

Developing a Siamese Network for Intrusion Detection Systems

Hanan Hindy
Division of Cyber Security, Abertay University
Dundee, Scotland, UK
hananhindy@ieee.org

Christos Tachtatzis
EEE Department, University of Strathclyde, Glasgow, Scotland, UK
Glasgow, Scotland, UK
christos.tachtatzis@strath.ac.uk

Robert Atkinson
EEE Department, University of Strathclyde, Glasgow, Scotland, UK
Glasgow, Scotland, UK
robert.atkinson@strath.ac.uk

Ethan Bayne
Division of Cyber Security, Abertay University
Dundee, Scotland, UK
e.bayne@abertay.ac.uk

Xavier Bellekens
EEE Department, University of Strathclyde, Glasgow, Scotland, UK
Glasgow, Scotland, UK
xavier.bellekens@strath.ac.uk

Abstract

Machine Learning (ML) for developing Intrusion Detection Systems (IDS) is a fast-evolving research area that has many unsolved domain challenges. Current IDS models face two challenges that limit their performance and robustness. Firstly, they require large datasets to train and their performance is highly dependent on the dataset size. Secondly, zero-day attacks demand that machine learning models are retrained in order to identify future attacks of this type. However, the sophistication and increasing rate of cyber attacks make retraining time prohibitive for practical implementation. This paper proposes a new IDS model that can learn from pair similarities rather than class discriminative features. Learning similarities requires less data for training and provides the ability to flexibly adapt to new cyber attacks, thus reducing the burden of retraining. The underlying model is based on Siamese Networks, therefore, given a number of instances, numerous similar and dissimilar pairs can be generated. The model is evaluated using three mainstream IDS datasets; CICIDS2017, KDD Cup'99, and NSL-KDD. The evaluation results confirm the ability of the Siamese Network model to suit IDS purposes by classifying cyber attacks based on similarity-based learning. This opens a new research direction for building adaptable IDS models using non-conventional ML techniques.

EuroMLSys '21, April 26, 2021, Online, United Kingdom

ACM ISBN 978-1-4503-8298-4/21/04…$15.00
https://doi.org/10.1145/3437984.3458842

CCS Concepts: • **Security and privacy → Intrusion detection systems**; **Network security**; • **Computing methodologies → Machine learning**; **Neural networks**.

Keywords: Intrusion Detection, Siamese Network, Artificial Neural Network, Few-Shot Learning, Machine Learning, CICIDS2017, KDD Cup'99, NSL-KDD.

ACM Reference Format:
Hanan Hindy, Christos Tachtatzis, Robert Atkinson, Ethan Bayne, and Xavier Bellekens. 2021. Developing a Siamese Network for Intrusion Detection Systems. In *The 1st Workshop on Machine Learning and Systems (EuroMLSys '21), April 26, 2021, Online, United Kingdom.* ACM, New York, NY, USA, 7 pages. https://doi.org/10.1145/3437984.3458842

1 Introduction

The number of cyber attacks is increasing at an exponential rate [23], hence, new, non-traditional techniques are required to cope with the increasing volume and variety of attacks. IDS development is comprised of three stages; statistical, knowledge-based, and ML [5, 7]. In all of these stages, large datasets are required as a building block. However, the lack of dataset availability and the difficulty of recording real-life scenarios hinders the advancement of IDS.

One approach to overcome the dataset availability problem is to build synthetic datasets with up-to-date attacks. However, this is a challenging task as it requires a considerable amount of time to find suitable representable environments and parameters. A second approach is to collect real-life datasets; however, this requires preprocessing, anonymization, and attack labelling as discussed in [20, 30].

In this paper, a new learning approach, based on One-Shot Learning - is proposed for designing and building IDS that can lean based on pairs similarity. To the best of the authors' knowledge, this approach has not been introduced for IDS before. A few attempts have been made at applying One-Shot for malware detection based on transforming malware to image-like structure and leveraging image-based

models [9, 31, 33]. One-Shot learning - unlike traditional learning techniques - requires few samples from each class to train on, therefore, overcoming the need for large datasets. The proposed model is designed based on 'Siamese Network'. Based on the Siamese Network learning paradigm, it is well suited as a One-Shot learning technique. Siamese Networks are trained to learn pair similarities rather than distinctive features for each class. A pair is composed of two instances and a similar or dissimilar label. Wang *et. al* define a training pair as "constituted by an exemplar and an instance, and response ground-truth" [36]. The presented architecture is evaluated based on how accurately the model can classify attacks based solely on similarity. This opens a research direction that leverages similarity-based learning to build flexible IDS. Three IDS benchmark datasets are used for evaluation.

The contributions of this paper are threefold:

- We propose a novel IDS approach based on One-Shot Learning, which to the best of the authors' knowledge, is the first application for IDS.
- We utilise a Siamese Network model to classify cyber attacks based on similarities. Therefore, this will reduce the dataset generation burden and help in developing IDSs that can cope with the new attack pace.
- We evaluate the proposed Siamese Network model on three benchmark IDS datasets; CICIDS2017, NSL-KDD and KDD Cup'99.

The rest of the paper is organised as follows; Section 2 explains the ML background to this manuscript, Section 3 discusses the proposed model architecture. Section 4 presents the experimental findings and analysis of the results. The key takeaways, limitations, and recommendations are presented in Section 5. Finally, the paper concludes in Section 6.

2 Related Work

ML techniques dominated the IDS research in the past decade. ML models can be supervised, unsupervised, or semi-supervised. ML models are trained for an intended use-case. For example, ML models can be trained to predict a certain output, classify classes, etc. ML relies on mathematical models for this training process. For this training process to be effective, large datasets are required.

Resolving the relation between the ML model size and the required amount of data has been a prominent research area in the past decade. This problem affects the development of robust and up-to-date IDS. Given the fact that publicly available datasets offer limited attack coverage, IDS development has suffered.

Datasets are often depicted as the bottleneck for developing robust ML models due to the following reasons [25]:

1. Gathering large realistic datasets is a complex task and requires a lot of manual labour.
2. Using synthetic or deprecated datasets makes it difficult for the developed model to fit in real-life deployments.
3. Training classical ML models with small datasets exposes the models to over-fitting problems.
4. Continuous generation of datasets to cope with emerging attacks.

To overcome the need to build new datasets for detecting unknown attacks, Sun *et al.* [29] proposed a Bayesian probabilistic model to detect Zero-Day attack paths. They visualised attacks in a graph-like structure and introduced a prototype to identify Zero-Day attacks. Lake *et al.* [14] proposed the use of probabilistic induction to generalise image learning techniques. The idea is based on mimicking human behaviour and their ability to generalise from one example.

Li *et. al* [15] discuss the large dataset requirements and the difficulty to obtain such datasets. Furthermore, traditional approaches require an extensive amount of time to train a single model. Online Learning provides a potential solution for these problems and focuses on reducing the computation time needed to adapt the model by updating the last layer weights [26], however, caution must be taken when utilising these approaches as models could shift to undesirable states. While viable, online learning is not suitable to learn from limited datasets, nor detect unknown attacks.

One-Shot learning focuses on learning new classes from only one - or few - examples. In this work, a One-Shot learning is applied to the intrusion detection problem and proposed a model that uses Siamese Networks to learn attack instance similarities.

One of the most popular ML techniques, and a building block of other ML models including Siamese Netowkes, is Artificial Neural Network (ANN). ANN is inspired by the human brain, thus its building block is the artificial neurons. An artificial neuron is composed of three (a) input, (b) output, and (c) activation function [37]. Typically, an ANN is composed of an input layer, an output layer, and zero or more hidden layers. Each of these layers is composed of multiple neurons. Neurons in each layer are connected to the ones in the following layer using connections called 'weights'.

An ANN is trained (the weights are adjusted) to best minimise the loss. Once the ANN is trained, the input neurons values are propagated using weights/connections and activation functions to correspond to the desired output [37]. Siamese Networks, as further discussed in Section 3, are built using two ANN networks. The two networks are called 'Twin' networks, which can be visualised in Figure 1-B.

Siamese Network usage has advanced in various domains. For example, Koch *et al.* [13] and Jiao *et al.* [11] developed it for image processing usage. Although Image and Video processing has been the prominent domain, Siamese Networks are used in the medical domain [1] and Natural Language Processing (NLP) domain [22, 38]. They have been used for

reducing dimensionality by Moustakidis and Karlsson [19]. To the best of the authors knowledge, this is the first proposed work using Siamese Networks to build IDS.

3 Proposed IDS Model

The proposed model leverages similarity-based learning and relies on a Siamese Network model. Bromley *et al.* [2] are the first to propose the use of Siamese Network for solving the problem of hand-written signatures matching. A Siamese Network is composed of two identical ANN called twin networks. These twin networks share the same weights and they train simultaneously. This network, unlike other ML techniques, is trained to decide whether a given pair is similar or not. The output is the degree of similarity which can also be squashed to a binary similar/dissimilar output.

Figure 1 visualises the overall process comprising three sub-processes. Figure 1-(A) is concerned with preparing datasets for training and evaluation. Having a dataset with N classes, each class is split into two parts. The first part is used for training and the second is used for testing (i.e., 50% for generating training pairs and 50% for generating testing pairs). Unlike traditional ML techniques, the training instances are not fed directly to the network to learn from. As aforementioned, Siamese Networks train to decide on pair similarity, thus the training samples are passed into the model as pairs with their labels 'similar' or 'dissimilar'. Using the first half of each class, similar and dissimilar pairs are randomly generated. The generation of pairs must ensure the following constraints: (a) The uniqueness of pairs (i.e., no duplicates). (b) The balanced representation of all combinations (i.e., equal number of pairs for each combination of similar and dissimilar pairs). (c) The number of classes (N) must be more than 2, otherwise the network will converge to a 50% similarity.

Once the training batch is generated, the Siamese Network is trained for n iterations (Figure 1-(B)). The value of n is chosen using ANN parameter optimisation. Based on the monitoring the training and validation loss curves, the number of iterations at which the network converges is chosen. For this study, $n = 2000$, which is decided by hyperparameter optimisation and monitoring the loss curves. The training uses Adam optimiser [12, 24] and the loss is calculated using Equation 1. This loss function is proposed by Chopra, Hadsell, and LeCun [4] and is called "constructive loss" where $(a, b)_i$ is the i^{th} pair in the batch B, $y(a, b)$ is the label (similar (1) or dissimilar (0)), d_i is the distance (similarity) calculated by the network and $m > 0$ is a margin. In this work, the margin is set to $m = 1$ [4]. The constructive loss is best suited for the Siamese network training since it limits the contribution of dissimilar pairs to the total loss if the difference exceeds m. Therefore, if the distance between the dissimilar pairs is large, it does not bias the overall loss.

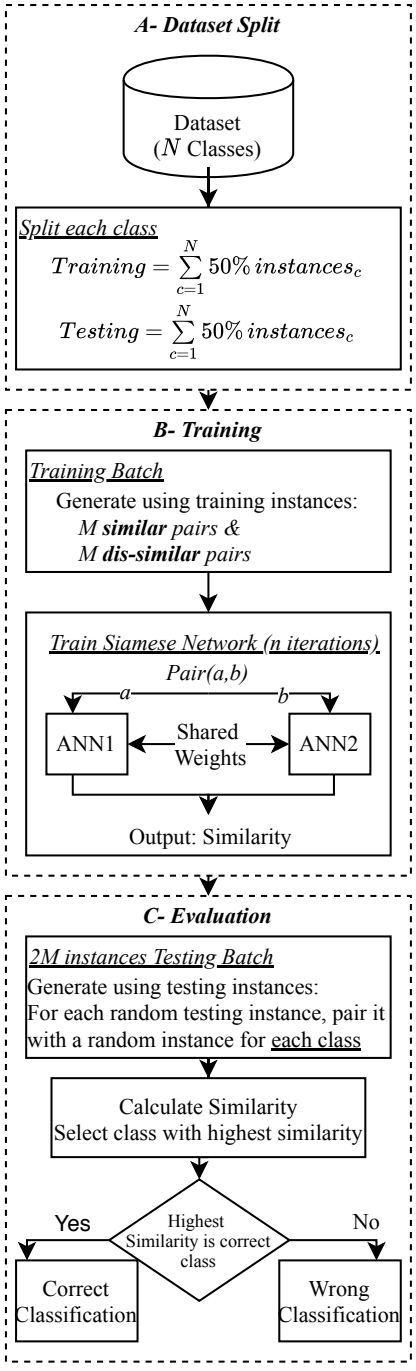

Figure 1. Proposed Similarity-Based IDS Model

$$loss = \sum_{i=1}^{B} y(a,b)_i * (d_i)^2 + (1 - y(a,b)_i) * (max(m - d_i, 0))^2 \quad (1)$$

Finally, the model is evaluated (Figure 1-(C)). Relying on the similarity check, the evaluation is performed as follows. Given a random testing instance x, the instance is paired

with a random instance from each class (i.e. For each $n \in N$, a pair (x, instance $\in n$) is used). The similarity of all pairs is calculated, and an instance x is given the classification label based on the class of the most similar pair (i.e., the closest pair). Since the pairing is based on randomness, multiple instances are used from each class and an aggregation method is used to get the classification label (i.e., given a random testing instance x, x is paired with a random instance from each class multiple times (j) and the results are aggregated using majority voting).

4 Experiments and Results

The model discussed in Section 3 is evaluated using three IDS benchmark datasets. These datasets are CICIDS2017 and NSL-KDD. Moreover, KDD Cup'99 is used in comparison to the NSL-KDD to assess the impact of having clean data when generating the pairs to train the model.

The CICIDS2017 dataset [28] is a recent dataset generated by the Canadian Institute for Cybersecurity (CIC). The CICIDS2017 dataset comprises up-to-date benign, insider, and outsider cyber attacks. Using the provided '.pcap' files, bidirectional flow features are generated and instances are labeled.

Although old, the KDD Cup'99 [6] is still considered the classic benchmark dataset used in evaluating IDS. More than 60% of the research in the past years (2008 - 2020) is evaluated using KDD'99 [7]. KDD Cup'99 covers 4 attack classes alongside normal activity. The attacks contained in the dataset are: Denial of Service (DoS), Root to Local (R2L), User to Root (U2R) and probing.

The KDD Cup'99 dataset is relatively large, however, the provider published a reduced subset of ~10% [34]. For the purposes of evaluation, only the smaller subset is used to ensure the applicability of the proposed Siamese Network to learn from limited data.

The NSL-KDD [3] dataset is proposed by the CIC to overcome the problems of the KDD Cup'99 dataset discussed by Tavallaee *et al.* [32]. Similar to KDD Cup'99, NSL-KDD covers 4 attack classes alongside normal activity. The NSL-KDD is used for evaluation to observe the effect of enhancing and filtering a dataset on the similarity learning and performance.

The NSL-KDD and KDD Cup'99 are already preprocessed and provided in 42 features. The CICIDS2017 has 31 bidirectional flow features.

As aforementioned, ANN is used as the building block of Siamese twin networks. The optimal netowrk architecture based on hyper parameter optimisation (number of hidden layers and neurons) for the datasets is (**bold**: input, *italic*: output of Siamese Network before similarity calculation, Dr: Dropout layer):

- CICIDS2017:
  31:25:Dr(0.1):20:Dr(0.05):*15*
- NSL-KDD - KDD Cup'99:
  118:98:Dr(0.1):79:Dr(0.1):59:Dr(0.1):39:Dr(0.1):*20*

4.1 CICIDS2017 Results

The Confusion Matrix (CM) of the classification for the CICIDS2017 is presented in Table 1. The results is obtained when $j = 5$ pairs are used. As demonstrated, based only on pair similarity, the overall accuracy is 83.74%, which rises to 84.71% when $j = 30$, as shown in Table 2. The different attack classes detection accuracies are 96.08%, 75.17%, 80.05% and 76.55% respectively. Moreover, the low false negatives are presented in the first column. Also, a low false positive rate for Normal (0.05%, 2.6%, 1.87% and 4.62%) for the attack classes, respectively.

Table 2 demonstrates the overall accuracy, TNR, and FPR when using different j pairs when aggregating the results using majority voting. Two observations are noted. (a) Using 5 pairs results in a distinctive rise compared to using 1 pair in both the overall accuracy (from 74.55% to 83.74%) and the TNR (from 70.43% to 90.87%). The is due to the instance selection randomness which has a high influence when only 1 pair is used. (b) Using more than 5 pairs improves the accuracy but with a small margin (~1%).

Table 1. CICIDS2017 Classification Confusion Matrix (5 pairs)

	Predicted Class					
Correct	Normal	DoS (Hulk)	DoS (Slowloris)	FTP	SSH	Overall
Normal	5452 **(90.87%)**	3 *(0.05%)*	156 *(2.6%)*	112 *(1.87%)*	277 *(4.62%)*	83.74%
DoS (Hulk)	139 *(2.32%)*	5765 **(96.08%)**	24 *(0.4%)*	13 *(0.22%)*	59 *(0.98%)*	
DoS (Slowloris)	914 *(15.23%)*	1 *(0.02%)*	4510 **(75.17%)**	71 *(1.18%)*	504 *(8.4%)*	
FTP	790 *(13.17%)*	2 *(0.03%)*	95 *(1.58%)*	4803 **(80.05%)**	310 *(5.17%)*	
SSH	973 *(16.22%)*	0 *(0%)*	227 *(3.78%)*	207 *(3.45%)*	4593 **(76.55%)**	

Table 2. CICIDS2017 Classification Accuracy Using Different j Votes

No Votes (j)	Overall Accuracy	Normal	
		TNR	FPR
1	74.55%	70.43%	29.57%
5	83.74%	90.87%	9.13%
10	84.54%	92.58%	7.42%
15	84.63%	93.07%	6.93%
20	84.69%	93.55%	6.45%
25	84.69%	93.73%	6.27%
30	84.71%	93.85%	6.15%

4.2 KDD Cup'99 and NSL-KDD Results

The CM of the classification for the KDD Cup'99 dataset is presented in Table 3. As shown, the overall accuracy is

87.99% with a small portion of malicious traffic misclassified as normal (0.1%, 0.97%, 0.27% and 8% for the attack classes, respectively).

Similar to the results presented in Section 4.1, using 5 pairs results in a rise in the accuracy and TNR as outlined in Table 4.

Table 3. KDD Cup'99 Classification Confusion Matrix (5 pairs)

	Predicted Class					
Correct	Normal	DoS	Probe	R2L	U2R	Overall
Normal	4423 **(73.72%)**	9 *(0.15%)*	492 *(8.2%)*	979 *(16.32%)*	97 *(1.62%)*	87.99%
DoS	6 *(0.1%)*	5920 **(98.67%)**	64 *(1.07%)*	10 *(0.17%)*	0 *(0%)*	
Probe	58 *(0.97%)*	254 *(4.23%)*	5453 **(90.88%)**	222 *(3.7%)*	13 *(0.22%)*	
R2L	16 *(0.27%)*	0 *(0%)*	39 *(0.65%)*	5786 **(96.43%)**	159 *(2.65%)*	
U2R	480 *(8%)*	0 *(0%)*	685 *(11.42%)*	21 *(0.35%)*	4814 **(80.23%)**	

Table 4. KDD Cup'99 Classification Accuracy Using Different j Votes

No Votes (j)	Overall Accuracy	Normal	
		TNR	FPR
1	82.03%	69.27%	30.73%
5	87.99%	73.72%	26.28%
10	88.26%	73.67%	26.33%
15	88.29%	73.63%	26.37%
20	88.26%	73.65%	26.35%
25	88.23%	73.6%	26.4%
30	88.24%	73.6%	26.4%

Training the Siamese Network model on the NSL-KDD dataset, which is an improved dataset based on the KDD Cup'99 (filtered and removed duplicates), did not show a significant rise in the classification results. This is owed to the randomness of pair selection and the Siamese Network learning approach. Since the Siamese Network learns from similarities, not specific class features, it can overcome the balancing and duplicate issues. The randomisation of choosing the training batch pairs and ensuring the balanced representation of class pairs conribute to this as well.

The CM of the NSL-KDD dataset is presented in Table 5. The overall accuracy increased to 91.01% with around the same False Negative rates.

Table 5. NSL-KDD Classification Confusion Matrix (5 pairs)

	Predicted Class					
Correct	Normal	DoS	Probe	R2L	U2R	Overall
Normal	5187 **(86.45%)**	47 *(0.78%)*	300 *(5%)*	315 *(5.25%)*	151 *(2.52%)*	91.01%
DoS	144 *(2.4%)*	5621 **(93.68%)**	217 *(3.62%)*	16 *(0.27%)*	2 *(0.03%)*	
Probe	159 *(2.65%)*	643 *(10.72%)*	5133 **(85.55%)**	44 *(0.73%)*	21 *(0.35%)*	
R2L	227 *(3.78%)*	0 *(0%)*	31 *(0.52%)*	5669 **(94.48%)**	73 *(1.22%)*	
U2R	214 *(3.57%)*	0 *(0%)*	92 *(1.53%)*	2 *(0.03%)*	5692 **(94.87%)**	

Table 6. NSL-KDD Classification Accuracy Using Different j Votes

No Votes (j)	Overall Accuracy	Normal	
		TNR	FPR
1	86.61%	80.47%	19.53%
5	91.01%	86.45%	13.55%
10	91.1%	86.45%	13.55%
15	91.17%	86.4%	13.6%
20	91.24%	86.47%	13.53%
25	91.26%	86.42%	13.58%
30	91.3%	86.53%	13.47%

It is important to note that, compared to recent deep learning models that classify cyber attack classes using feature learning, the Siamese Network model demonstrates its effectiveness. KDD Cup'99 overall accuracy using the Siamese network model reaches 88% compared to 92.6% in [35] and 99.8% in [27]. However, based solely on similarity-based learning, the true positive rates are 98.67%, 90.88%, 96.43%, and 80.23% for DoS, Probe, R2L and U2R, respectively. These results outperform the use of ANNs in [35] where the detection rates for the same attack classes are 93.9%, 73.2%, 24.3%, and 15.5% and 99.9%, 98.9%, 96.9%, and 75% in [27].

Similarly, for the NSL-KDD dataset, recent research reported an overall accuracy of 83.83% when using an ensemble DL model [10] and 77.8% in [35], while the overall accuracy reported in this paper is 91.01%, with a detection rate of 93.68%, 85.55%, 94.48%, and 94.87% for the attack classes respectively. Another paper [16] that uses a convolution neural network to classify attacks in the NSL-KDD dataset, reports a true posite rate of 86.63% for DoS, 83.73% for Probe, 35.15% for R2L, and 23.50% for U2R, compared to 93.68%, 85.55%, 94.48%, and 94.87% in this work.

Finally, the CICIDS2017 overall accuracy reaches 84% using the Siamese network model, compared with 96% in [8]. The true posite rate of FTP and SSH classes is 80.05% and 76.55% compared with 98% and 77% in [8] and 0% and 3.1% in [35].

5 Discussion and Limitations

In this section, the main takeaways are discussed, based on the proposed model in Section 3 and the results presented in Section 4. Limitations and recommendations of using Siamese Network are provided.

5.1 Key Takeaways

- **Datasets Usage**: Siamese Networks prove their ability to learn from pairs similarity, thus the ability to learn from few instances. This lessens the burden of collecting large amounts of data and labelling it. Secondly, it accelerates the process of having an IDS model trained to classify new attacks.
- **Classes' Representatives**: The optimal method of choosing instances to represent each class to accelerate the training and evaluation processes solely depending on pairs is still a known and open research question in literature [18]. Therefore, instead of choosing random instances to calculate similarity, class representatives could be used.
- **Classes' Representatives Randomness**: Since the evaluation of the Siamese Network is based on selecting random pairs, it is recommended to choose multiple random instances from each class. Voting is then used to aggregate the results.
- **Class Instances Distinctiveness**: To ensure the correctness of the similarity learning, instances that are collected from each attack class and normal scenarios should be distinctive. The more distinctive the class instances are, the more effective the Siamese Network will be at detection.

5.2 Limitations

- **Pairs Selection**: When generating training batches for the Siamese Networks, it is key to identify the best pairing technique. Training with all pairs combinations is often not practical. Current research uses a random choice of pairs with the constraint of having an equal number of similar and dissimilar pairs. However, a choice of more distinctive pairs could enhance the accuracy of the model and accelerate its convergence.
- **Finding ANN Architecture**: Finding a suitable ANN architecture could be challenging. An architecture that suits one dataset might not suit another, however, the modality of the model presented in this paper renders it extendable and not tightly coupled with a particular ANN architecture. Furthermore, grid search or random search can be used to identify the optimal parameters [17].

6 Conclusion and Future Work

This paper proposed a novel Siamese Network-based model for IDS. The model leverages similarity-based learning to enable training using limited instances and allows the applicability of building flexible IDS. This is the first IDS model based on One-Shot learning and similarity-based learning. Given a dataset, the model is trained using pairs and is used to classify cyber attacks. The model is evaluated using three IDS benchmark datasets, namely; CICIDS2017, NSL-KDD and KDD Cup'99.

In the experiments, a careful consideration must be given when creating the training set, ensuring an equal number of training pairs for every class combination. This, in turn, brought its own challenges with an exploding number of combinations between all instances. To minimise this effect, distinct pairs were chosen to create large batches in the region of 30,000 pairs [13, 21]. During the evaluation, similarity comparison using a single point for each class resulted in noisy predictions due to randomness. This behaviour was avoided by choosing multiple random instances from each class and aggregating using majority voting.

The results of the Siamese Network demonstrated high classification performance. The similarity-based model was able to classify with an accuracy reaching 84% for the CICIDS2017, 88% for the KDD Cup'99 while for the NSL-KDD the accuracy reached over 91%. Although the proposed method classify attacks based on similarity only, compared to other ML techniques that train on class discriminative features, the Siamese Network classification performance falls inline with recent research.

These results demonstrate the ability of the proposed architecture to learn from similarities. This opens a new research direction for IDS that can adapt to new cyber attacks.

Future work involves evaluating the models using other datasets. Moreover, proposing other applications for One-Shot learning in the Cyber-Security domain. The code will be made available through a GitHub repository.

References

[1] Anuja Kumar Acharya and Rajalakshmi Satapathy. 2020. A Deep Learning Based Approach towards the Automatic Diagnosis of Pneumonia from Chest Radio-Graphs. *Biomedical and Pharmacology Journal* 13, 1 (2020), 449–455.

[2] Jane Bromley, Isabelle Guyon, Yann LeCun, Eduard Säckinger, and Roopak Shah. 1994. Signature Verification using a "Siamese" Time Delay Neural Network. In *Advances in Neural Information Processing Systems*. 737–744.

[3] Canadian Institute for Cybersecurity. [n.d.]. NSL-KDD dataset. http://www.unb.ca/cic/datasets/nsl.html Accessed on 15/06/2018).

[4] Raia Hadsell, Sumit Chopra, and Yann LeCun. 2006. Dimensionality Reduction by Learning an Invariant Mapping.. In *2006 IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR'06)*, Vol. 2. IEEE, 1735–1742.

[5] Tarfa Hamed, Jason B Ernst, and Stefan C Kremer. 2018. A Survey and Taxonomy of Classifiers of Intrusion Detection Systems. In *Computer and Network Security Essentials*. Springer, 21–39.

[6] S. Hettich and S. D. Bay. 1999. The UCI KDD Archive. http://kdd.ics.uci.edu (Accessed on 06/15/2018).

[7] H. Hindy, D. Brosset, E. Bayne, A. K. Seeam, C. Tachtatzis, R. Atkinson, and X. Bellekens. 2020. A Taxonomy of Network Threats and the Effect of Current Datasets on Intrusion Detection Systems. *IEEE Access* 8 (2020), 104650–104675.

[8] Md Delwar Hossain, Hideya Ochiai, Fall Doudou, and Youki Kadobayashi. 2020. SSH and FTP Brute-force Attacks Detection in Computer Networks: LSTM and Machine Learning Approaches.. In *5th International Conference on Computer and Communication Systems (ICCCS)*. IEEE, 491–497. https://doi.org/10.1109/ICCCS49078.2020.9118459

[9] Shou-Ching Hsiao, Da-Yu Kao, Zi-Yuan Liu, and Raylin Tso. 2019. Malware image classification using one-shot learning with siamese networks. *Procedia Computer Science* 159 (2019), 1863–1871.

[10] Poulmanogo Illy, Georges Kaddoum, Christian Miranda Moreira, Kuljeet Kaur, and Sahil Garg. 2019. Securing Fog-to-Things Environment Using Intrusion Detection System Based On Ensemble Learning.. In *2019 IEEE Wireless Communications and Networking Conference (WCNC)* (Marrakesh, Morocco). IEEE, 1–7. https://doi.org/10.1109/WCNC.2019.8885534

[11] Shanshan Jiao, Jiabao Wang, Zhisong Pan, Guyu Hu, Junhua Zou, and Mingyong Zeng. 2019. Multi-layer Joint Classification-Metric Deep Learning for Top View Image Person Re-identification. In *2019 IEEE 2nd International Conference on Electronics and Communication Engineering (ICECE)*. IEEE, 47–50.

[12] Diederik P. Kingma and Jimmy Ba. 2015. Adam: A Method for Stochastic Optimization. In *3rd International Conference on Learning Representations, ICLR 2015, San Diego, CA, USA, May 7-9, 2015, Conference Track Proceedings*, Yoshua Bengio and Yann LeCun (Eds.). http://arxiv.org/abs/1412.6980

[13] Gregory Koch, Richard Zemel, and Ruslan Salakhutdinov. 2015. Siamese Neural Networks for One-Shot Image Recognition. In *ICML Deep Learning Workshop*, Vol. 2.

[14] Brenden M. Lake, Ruslan Salakhutdinov, and Joshua B. Tenenbaum. 2015. Human-level Concept Learning through Probabilistic Program Induction. *Science* 350, 6266 (2015), 1332–1338.

[15] Bingdong Li, Jeff Springer, George Bebis, and Mehmet Hadi Gunes. 2013. A Survey of Network Flow Applications. *Journal of Network and Computer Applications* 36, 2 (2013), 567–581.

[16] Yanmiao Li, Yingying Xu, Zhi Liu, Haixia Hou, Yushuo Zheng, Yang Xin, Yuefeng Zhao, and Lizhen Cui. 2020. Robust Detection for Network Intrusion of Industrial IoT based on Multi-CNN Fusion. *Measurement* 154 (2020), 107450. https://doi.org/10.1016/j.measurement.2019.107450

[17] Petro Liashchynskyi and Pavlo Liashchynskyi. 2019. Grid Search, Random Search, Genetic Algorithm: A Big Comparison for NAS. *arXiv preprint arXiv:1912.06059* (2019).

[18] Xialei Liu, Joost van de Weijer, and Andrew D. Bagdanov. 2017. RankIQA: Learning From Rankings for No-Reference Image Quality Assessment. In *The IEEE International Conference on Computer Vision (ICCV)*.

[19] Serafeim Moustakidis and Patrik Karlsson. 2020. A novel feature extraction methodology using Siamese convolutional neural networks for intrusion detection. *Cybersecurity* 3, 1 (2020), 1–13.

[20] Maël Nogues, David Brosset, Hanan Hindy, Xavier Bellekens, and Yvon Kermarrec. 2020. Labelled Network Capture Generation for Anomaly Detection. In *Foundations and Practice of Security*, Abdelmalek Benzekri, Michel Barbeau, Guang Gong, Romain Laborde, and Joaquin Garcia-Alfaro (Eds.). Springer International Publishing, Cham, 98–113.

[21] S. Pang, S. Qiao, T. Song, J. Zhao, and P. Zheng. 2019. An Improved Convolutional Network Architecture Based on Residual Modeling for Person Re-Identification in Edge Computing. *IEEE Access* 7 (2019), 106749–106760.

[22] Nuttachot Promrit, Sajjaporn Waijanya, and Kran Thaweesith. 2019. The Evaluation of Thai Poem's Content Consistency using Siamese Network. In *Proceedings of the 2019 3rd International Conference on Natural Language Processing and Information Retrieval*. 115–120.

[23] Ullas P Ramakrishnan and JK Tandon. 2018. The Evolving Landscape of Cyber Threats. *Vidwat* 11, 1 (2018), 31–35.

[24] Sashank J. Reddi, Satyen Kale, and Sanjiv Kumar. 2018. On the Convergence of Adam and Beyond. In *International Conference on Learning Representations*. https://openreview.net/forum?id=ryQu7f-RZ

[25] Yuji Roh, Geon Heo, and Steven Euijong Whang. 2021. A survey on data collection for machine learning: a big data-ai integration perspective. *IEEE Transactions on Knowledge and Data Engineering* 33, 4 (2021), 1328–1347.

[26] Setareh Roshan, Yoan Miche, Anton Akusok, and Amaury Lendasse. 2018. Adaptive and Online Network Intrusion detection system using clustering and Extreme Learning Machines. *Journal of the Franklin Institute* 355, 4 (2018), 1752–1779.

[27] Martin Sarnovsky and Jan Paralic. 2020. Hierarchical Intrusion Detection using Machine Learning and Knowledge Model. *Symmetry* 12, 2 (2020), 203. https://doi.org/10.3390/sym12020203

[28] Iman Sharafaldin, Arash Habibi Lashkari, and Ali A. Ghorbani. 2018. Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization.. In *ICISSP*. SciTePress, 108–116. https://doi.org/10.5220/0006639801080116

[29] X. Sun, J. Dai, P. Liu, A. Singhal, and J. Yen. 2018. Using Bayesian Networks for Probabilistic Identification of Zero-Day Attack Paths. *IEEE Transactions on Information Forensics and Security* 13, 10 (2018), 2506–2521. https://doi.org/10.1109/TIFS.2018.2821095 ID: 1.

[30] Muhammad Tahir, Mingchu Li, Naeem Ayoub, and Muhammad Aamir. 2019. Efficacy Improvement of Anomaly Detection by Using Intelligence Sharing Scheme. *Applied Sciences* 9, 3 (2019), 364.

[31] Zhijie Tang, Peng Wang, and Junfeng Wang. 2020. ConvProtoNet: Deep prototype induction towards better class representation for few-shot malware classification. *Applied Sciences* 10, 8 (2020), 2847.

[32] Mahbod Tavallaee, Ebrahim Bagheri, Wei Lu, and Ali A. Ghorbani. 2009. A Detailed Analysis of the KDD CUP 99 Data Set.. In *2009 IEEE Symposium on Computational Intelligence for Security and Defense Applications* (Ottawa, ON, Canada). IEEE, 1–6. https://doi.org/10.1109/CISDA.2009.5356528

[33] Trung Kien Tran, Hiroshi Sato, and Masao Kubo. 2019. Image-based unknown malware classification with few-shot learning models. In *2019 Seventh International Symposium on Computing and Networking Workshops (CANDARW)*. IEEE, 401–407.

[34] UCI. 1999. KDD Cup 1999 Data. http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html. (Accessed on 12/07/2018).

[35] R. Vinayakumar, Mamoun Alazab, K. P. Soman, Prabaharan Poornachandran, Ameer Al-Nemrat, and Sitalakshmi Venkatraman. 2019. Deep Learning Approach for Intelligent Intrusion Detection System. *IEEE Access* 7 (2019), 41525–41550. https://doi.org/10.1109/ACCESS.2019.2895334

[36] Qiang Wang, Zhu Teng, Junliang Xing, Jin Gao, Weiming Hu, and Stephen Maybank. 2018. Learning Attentions: Residual Attentional Siamese Network for High Performance Online Visual Tracking. In *The IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*. IEEE, 4854–4863.

[37] Bill Wilson. 2018. The Machine Learning Dictionary. https://web.archive.org/web/20180826151959/http://www.cse.unsw.edu.au/~billw/mldict.html (Accessed on 06/29/2020).

[38] Yujia Wu, Jing Li, Jia Wu, and Jun Chang. 2020. Siamese capsule networks with global and local features for text classification. *Neurocomputing* 390 (2020), 88–98.