```
@inproceedings{Abolhasanzadeh2015,
	Abstract = {The continuous advances in technology is the reason of integration of our lives and
information systems. Due to this fact the importance of security in these systems increases. Therefore, the
application of intrusion detection systems as security solutions is increasing year by year. These systems
(IDSs) are considered as a way of protection against cyber-attacks. However, handling big data constitutes
one of the main challenges of intrusion detection systems and is the reason of low performance of these
systems from the view of time and space complexity. To address these problems we have proposed an
approach to reduce this complexity. Our approach is based on dimensionality reduction and the neural
network bottleneck feature extraction is considered as the main method in this research. We have conducted
several experiments on a benchmark dataset (NSL-KDD) to investigate the effectiveness of our approach.
The results show that our approach is promising in terms of accuracy for real-world intrusion detection.},
	Author = {Abolhasanzadeh, Bahareh},
	Booktitle = {2015 7th Conference on Information and Knowledge Technology, IKT 2015},
	Doi = {10.1109/IKT.2015.7288799},
	File = {:Users/pooria/Downloads/07288799.pdf:pdf},
	Isbn = {9781467374859},
	Keywords = {Bottleneck Features,dimensionality reduction,intrusion detection},
	Month = {may},
	Pages = {1--5},
	Publisher = {IEEE},
	Title = {{Nonlinear dimensionality reduction for intrusion detection using auto-encoder bottleneck
features}},
	Url = {http://ieeexplore.ieee.org/document/7288799/},
	Year = {2015},
	Bdsk-Url-1 = {http://ieeexplore.ieee.org/document/7288799/},
	Bdsk-Url-2 = {http://dx.doi.org/10.1109/IKT.2015.7288799}}

@inproceedings{Alom2015,
	Abstract = {With the advent of digital technology, security threats for computer networks have increased
dramatically over the last decade being much bolder and brazen. There is a great need for an effective
Intrusion Detection System (IDS) which are intelligent specialized system designed to interpret the intrusion
attempts in incoming network traffic. Deep belief neural (DBN) networks proved to be the most influential
deep neural nets and generative neural networks that stack Restricted Boltzmann Machines. In this paper,
we explore the capabilities of DBN's performing intrusion detection through series of experiments after
training it with NSL-KDD dataset. The trained DBN network now identifies any kind of unknown attack in
dataset supplied to it and to the best of our knowledge this is first comprehensive paper performing intrusion
detection using deep belief nets. The proposed system not only detect attacks but also classify them in five
groups with the accuracy of identifying and classifying network activity based on limited, incomplete, and
nonlinear data sources. The proposed system achieved detection accuracy about 97.5{\%} for only fifty
iterations that is state of art performance compare to the existing system till today for intrusion detection.},
	Annote = {Very bullshit paper !},
	Author = {Alom, Md. Zahangir and Bontupalli, VenkataRamesh and Taha, Tarek M.},
	Booktitle = {2015 National Aerospace and Electronics Conference (NAECON)},
	Doi = {10.1109/NAECON.2015.7443094},
	File = {:Users/pooria/Downloads/07443094.pdf:pdf},
	Isbn = {978-1-4673-7565-8},
	Issn = {23792027},
	Keywords = {Computers,Deep packet inspection,Intrusion detection,KDD dataset,Monitoring,Neural
network,Neural networks,Telecommunication traffic,Training,deep belief nets,intrusion detection},
	Month = {jun},
	Pages = {339--344},
	Publisher = {IEEE},
	Title = {{Intrusion detection using deep belief networks}},
	Url = {http://ieeexplore.ieee.org/document/7443094/ http://ieeexplore.ieee.org/xpls/icp.jsp?arnumber=7443094{\%}5Cnhttp://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=7443094},
	Year = {2015},
	Bdsk-Url-1 = {http://dx.doi.org/10.1109/NAECON.2015.7443094}}

@article{Anselmi2016,
	Abstract = {The present phase of Machine Learning is characterized by supervised learning algorithms relying on large sets of labeled examples (. n??????). The next phase is likely to focus on algorithms capable of learning from very few labeled examples (. n???1), like humans seem able to do. We propose an approach to this problem and describe the underlying theory, based on the unsupervised, automatic learning of a "good" representation for supervised learning, characterized by small sample complexity. We consider the case of visual object recognition, though the theory also applies to other domains like speech. The starting point is the conjecture, proved in specific cases, that image representations which are invariant to translation, scaling and other transformations can considerably reduce the sample complexity of learning. We prove that an invariant and selective signature can be computed for each image or image patch: the invariance can be exact in the case of group transformations and approximate under non-group transformations. A module performing filtering and pooling, like the simple and complex cells described by Hubel and Wiesel, can compute such signature. The theory offers novel unsupervised learning algorithms for "deep" architectures for image and speech recognition. We conjecture that the main computational goal of the ventral stream of visual cortex is to provide a hierarchical representation of new objects/images which is invariant to transformations, stable, and selective for recognition-and show how this representation may be continuously learned in an unsupervised way during development and visual experience.},
	Archiveprefix = {arXiv},
	Arxivid = {1311.4158},
	Author = {Anselmi, Fabio and Leibo, Joel Z. and Rosasco, Lorenzo and Mutch, Jim and Tacchetti, Andrea and Poggio, Tomaso},
	Doi = {10.1016/j.tcs.2015.06.048},
	Eprint = {1311.4158},
	File = {:Users/pooria/Downloads/Anselmi2015.pdf:pdf},
	Issn = {03043975},
	Journal = {Theoretical Computer Science},
	Keywords = {Convolutional networks,Cortex,Hierarchy,Invariance},
	Pages = {112--121},
	Pmid = {18056803},
	Publisher = {Elsevier B.V.},
	Title = {{Unsupervised learning of invariant representations}},
	Url = {http://dx.doi.org/10.1016/j.tcs.2015.06.048},
	Volume = {633},
	Year = {2016},
	Bdsk-Url-1 = {http://dx.doi.org/10.1016/j.tcs.2015.06.048}}

@article{Bartos2016,
	Abstract = {New and unseen polymorphic malware, zero-day attacks, or other types of advanced persistent threats are usually not detected by signature-based security devices, fire-walls, or anti-viruses. This represents a challenge to the network security industry as the amount and vari-ability of incidents has been increasing. Consequently, this complicates the design of learning-based detection systems relying on features extracted from network data. The problem is caused by different joint distribution of observation (features) and labels in the training and test-ing data sets. This paper proposes a classification sys-tem designed to detect both known as well as previously-unseen security threats. The classifiers use statistical feature representation computed from the network traf-fic and learn to recognize malicious behavior. The rep-resentation is designed and optimized to be invariant to the most common changes of malware behaviors. This is achieved in part by a feature histogram constructed for each group of HTTP flows (proxy log records) of a user visiting a particular hostname and in part by a fea-ture self-similarity matrix computed for each group. The parameters of the representation (histogram bins) are op-timized and learned based on
```

the training samples along with the classifiers. The proposed classification system was deployed on large corporate networks, where it de-tected 2,090 new and unseen variants of malware sam-ples with 90{\%} precision (9 of 10 alerts were malicious), which is a considerable improvement when compared to the current flow-based approaches or existing signature-based web security devices.},
	Annote = {read 32
read 8
read 24
read 43
read conditional shift!
26 dataset

On the other hand, anomaly- based IDS systems are designed to detect wide range of network anomalies including yet undiscovered attacks, but at the expense of higher false alarm rates [8].

Invariantness of features learned by autoencoder? or any other generative model},
	Author = {Bartos, Karel and Sofka, Michal and Franc, Vojtech},
	File = {:Users/pooria/Downloads/sec16{_}paper{_}bartos.pdf:pdf},
	Isbn = {978-1-931971-32-4},
	Journal = {USENIX Security Symposium},
	Pages = {807--822},
	Title = {{Optimized Invariant Representation of Network Traffic for Detecting Unseen Malware Variants}},
	Url = {https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/bartos},
	Year = {2016},
	Bdsk-Url-1 = {https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/bartos}}

@article{Brauckhoff2009,
	Abstract = {Spatial Principal Component Analysis (PCA) has been proposed for network-wide anomaly detection. A recent work has shown that PCA is very sensitive to calibration settings. Unfortunately, the authors did not provide further explanations for this observation. In this paper, we fill this gap and provide the reasoning behind the found discrepancies. We revisit PCA for anomaly detection and evaluate its performance on our data. We develop a slightly modified version of PCA that uses only data from a single router. Instead of correlating data across different spatial measurement points, we correlate the data across different metrics. With the help of the analyzed data, we explain the pitfalls of PCA and underline our argumentation with measurement results. We show that the main problem is that PCA fails to capture temporal correlation. We propose a solution to deal with this problem by replacing PCA with the Karhunen-Loeve transform. We find that when we consider temporal correlation, anomaly detection results are significantly improved.},
	Annote = {Awesome theoratical paper about problems with PCA.
They have mentioned classic PCA cannot address temporal properties of network flow, and in return they have extended the idea of PCA to handle temporal properties

Very solid paper ... that requires multiple reading, I didn't underestand the math part as I just skimmed through},
	Author = {Brauckhoff, Daniela and Salamatian, Kave and May, Martin},
	Doi = {10.1109/INFCOM.2009.5062248},
	File = {:Users/pooria/Downloads/05062248.pdf:pdf},
	Isbn = {9781424435135},
	Issn = {0743166X},
	Journal = {Proceedings - IEEE INFOCOM},
	Keywords = {Applying PCA for Traffic Anomaly Detection: Proble},
	Pages = {2866--2870},
	Title = {{Applying PCA for traffic anomaly detection: Problems and solutions}},

```
	Year = {2009},
	Bdsk-Url-1 = {http://dx.doi.org/10.1109/INFCOM.2009.5062248}}

@article{Buczak2015,
	Abstract = {This survey paper describes a focused literature survey of machine learning (ML) and data mining (DM) methods for cyber analytics in support of intrusion detection. Short tutorial descriptions of each ML/DM method are provided. Based upon the number of citations or the relevance of an emerging method, papers representing each method were identified, read, and summarized. Because data are so important in ML/DM approaches, some well-known cyber data sets used in ML/DM are described. The complexity of ML/DM algorithms is addressed, discussion of challenges for using ML/DM for cyber security is presented, and some recommendations on when to use a given method are provided.},
	Annote = {One of the best written surveys that has broken every method to both use of misuse deteciton vs anamoly detection

83,84 hmm},
	Author = {Buczak, A and Guven, Erhan},
	Doi = {10.1109/COMST.2015.2494502},
	File = {:Users/pooria/Downloads/07307098.pdf:pdf},
	Isbn = {1553-877X VO - PP},
	Issn = {1553-877X},
	Journal = {IEEE Communications Surveys {\&} Tutorials},
	Keywords = {Computer security,Cyber Analytics,Data Mining,Data mining,Data models,IP networks,Machine Learning,Measurement,Ports (Computers),Protocols},
	Number = {99},
	Pages = {1},
	Title = {{A survey of data mining and machine learning methods for cyber security intrusion detection}},
	Volume = {PP},
	Year = {2015},
	Bdsk-Url-1 = {http://dx.doi.org/10.1109/COMST.2015.2494502}}

@article{Cheng2012,
	Abstract = {Detecting attacks disguised by evasion techniques is a challenge for signature-based Intrusion Detection Systems (IDSs) and Intrusion Prevention Systems (IPSs). This study examines five common evasion techniques to determine their ability to evade recent systems. The denial-of-service (DoS) attack attempts to disable a system by exhausting its resources. Packet splitting triestochop dataintosmall packets, so that a system may not completely reassemble the packets for signature matching. Duplicate insertion can mislead a system if the system and the target host discard different TCP/IP packets with a duplicate offset or sequence. Payload mutation fools a system with a mutative payload. Shellcode mutation transforms an attacker's shellcode to escape signature detection. This study assesses the effectiveness of these techniques on three recent signature-based systems, and among them, explains why Snort can be evaded. The results indicate that duplicate insertion becomes less effective on recent systems, but packet splitting, payload mutation and shellcode mutation can be still effective against them.},
	Annote = {Packet Splitting is a form of attack against signiture matching IDS},
	Author = {Cheng, Tsung Huan and Lin, Ying Dar and Lai, Yuan Cheng and Lin, Po Ching},
	Doi = {10.1109/SURV.2011.092311.00082},
	File = {:Users/pooria/Downloads/06042389.pdf:pdf},
	Isbn = {1553-877X},
	Issn = {1553877X},
	Journal = {IEEE Communications Surveys and Tutorials},
	Keywords = {Attacks,Evasion,IDS/IPS,Signature},
	Number = {4},
	Pages = {1011--1020},
	Pmid = {315392500005},
	Title = {{Evasion techniques: Sneaking through your intrusion detection/prevention systems}},
	Volume = {14},
	Year = {2012},
	Bdsk-Url-1 = {http://dx.doi.org/10.1109/SURV.2011.092311.00082}}

@article{Fiore2013,
	Abstract = {With the rapid growth and the increasing complexity of network infrastructures and the
evolution of attacks, identifying and preventing network abuses is getting more and more strategic to ensure
an adequate degree of protection from both external and internal menaces. In this scenario many techniques
are emerging for inspecting network traffic and discriminating between anomalous and normal behaviors to
detect undesired or suspicious activities. Unfortunately, the concept of normal or abnormal network behavior
depends on several factors and its recognition requires the availability of a model aiming at characterizing
current behavior, based on a statistical idealization of past events. There are two main challenges when
generating the training data needed for effective modeling. First, network traffic is very complex and
unpredictable, and second, the model is subject to changes over time, since anomalies are continuously
evolving. As attack techniques and patterns change, previously gained information about how to tell them
apart from normal traffic may be no longer valid. Thus, a desirable characteristic of an effective model for
network anomaly detection is its ability to adapt to change and to generalize its behavior to multiple different
network environments. In other words, a self-learning system is needed. This suggests the adoption of
machine learning techniques to implement semi-supervised anomaly detection systems where the classifier
is trained with "normal" traffic data only, so that knowledge about anomalous behaviors can be constructed
and evolve in a dynamic way. For this purpose we explored the effectiveness of a detection approach based
on machine learning, using the Discriminative Restricted Boltzmann Machine to combine the expressive
power of generative models with good classification accuracy capabilities to infer part of its knowledge from
incomplete training data. ?? 2013 Elsevier B.V.},
	Annote = {24,25 immune system

read26*

Very great paper that has used RBM

a nonparametric method is not based on any known
form or distribution of the sample observations and consequently
it is more robust.},
	Author = {Fiore, Ugo and Palmieri, Francesco and Castiglione, Aniello and {De Santis}, Alfredo},
	Doi = {10.1016/j.neucom.2012.11.050},
	File = {:Users/pooria/Library/Application Support/Mendeley Desktop/Downloaded/Fiore et al. - 2013 -
Network anomaly detection with the restricted Boltzmann machine.pdf:pdf},
	Issn = {09252312},
	Journal = {Neurocomputing},
	Keywords = {Anomaly detection,Energy-based models,Intrusion detection,Restricted Boltzmann
machine,Semi-supervised learning},
	Pages = {13--23},
	Title = {{Network anomaly detection with the restricted Boltzmann machine}},
	Volume = {122},
	Year = {2013},
	Bdsk-Url-1 = {http://dx.doi.org/10.1016/j.neucom.2012.11.050}}

@article{For2011,
	Annote = {NULL},
	Archiveprefix = {arXiv},
	Arxivid = {arXiv:1611.01726v1},
	Author = {For, Ethod},
	Eprint = {arXiv:1611.01726v1},
	File = {:Users/pooria/Downloads/1611.01726.pdf:pdf},
	Pages = {1--12},
	Title = {{H OST -B ASED I NTRUSION D ETECTION S YSTEMS}},
	Year = {2011}}

@article{Garcia-Teodoro2009,
	Abstract = {Anomaly detection IDS systems and platforms Assessment a b s t r a c t The Internet and computer networks are exposed to an increasing number of security threats. With new types of attacks appearing continually, developing flexible and adaptive security oriented approaches is a severe challenge. In this context, anomaly-based network intrusion detection techniques are a valuable technology to protect target systems and networks against malicious activities. However, despite the variety of such methods described in the literature in recent years, security tools incorporating anomaly detection functionalities are just starting to appear, and several important problems remain to be solved. This paper begins with a review of the most well-known anomaly-based intrusion detection techniques. Then, available platforms, systems under development and research projects in the area are presented. Finally, we outline the main challenges to be dealt with for the wide scale deployment of anomaly-based intrusion detectors, with special emphasis on assessment issues.},
	Author = {Garc{\'{i}}a-Teodoro, P. and D{\'{i}}az-Verdejo, J. and {Maci{\'{a}}-Fern{\'{a}} Ndez}, G and {V{\'{a}} Zquez}, E},
	Doi = {10.1016/j.cose.2008.08.003},
	File = {:Users/pooria/Library/Application Support/Mendeley Desktop/Downloaded/Garc{\'{i}}a-Teodoro et al. - 2009 - Anomaly-based network intrusion detection Techniques, systems and challenges.pdf:pdf},
	Isbn = {0167-4048},
	Issn = {01674048},
	Journal = {Computers {\&} Security},
	Keywords = {Anomaly detection,Assessment,IDS systems and platforms,Intrusion detection,Network security,Threat},
	Number = {1},
	Pages = {18--28},
	Title = {{Anomaly-based network intrusion detection: Techniques, systems and challenges}},
	Volume = {28},
	Year = {2009},
	Bdsk-Url-1 = {http://dx.doi.org/10.1016/j.cose.2008.08.003}}

@misc{Ghorbani2010,
	Abstract = {Intrusion Detection and Prevention is a rapidly growing field that deals with detecting and responding to malicious network traffic and computer misuse. Intrusion detection is the process of identifying and (possibly) responding to malicious activities targeted at computing and network resources. Any hardware or software automation that monitors, detects or responds to events occurring in a network or on a host computer is considered relevant to the intrusion detection approach. Different intrusion detection systems provide varying functionalities and benefits. Network Intrusion Detection and Prevention: Concepts and Techniques provides detailed and concise information on different types of attacks, theoretical foundation of attack detection approaches, implementation, data collection, evaluation, and intrusion response. Additionally, it provides an overview of some of the commercially/publicly available intrusion detection and response systems--Cover.},
	Annote = {read 19 : Packet header anomaly detection
read 7,8,3,17 for Connection Features
Ghorbani proposed in [26, 25] a Fuzzy Feature Eval- uation Framework for Network Intrusion Detection},
	Author = {Ghorbani, Ali A and Lu, Wei and Tavallaee, Mahbod},
	Booktitle = {{\ldots} and Autonomous System},
	Doi = {10.1007/978-0-387-88771-5},
	File = {:Users/pooria/Downloads/bok{\%}3A978-0-387-88771-5.pdf:pdf},
	Isbn = {978-0-387-88770-8},
	Issn = {15682633},
	Pages = {212},
	Title = {{Network Intrusion Detection and Prevention}},
	Url = {http://link.springer.com/10.1007/978-0-387-88771-5},
	Volume = {47},
	Year = {2010},
	Bdsk-Url-1 = {http://link.springer.com/10.1007/978-0-387-88771-5},
	Bdsk-Url-2 = {http://dx.doi.org/10.1007/978-0-387-88771-5}}

@article{Golovko2007,
	Author = {Golovko, Vladimir A. and Vaitsekhovich, Leanid U. and Kochurko, Pavel A. and Rubanau,
Uladzimir S.},
	Doi = {10.1109/IJCNN.2007.4371391},
	File = {:Users/pooria/Downloads/04371391.pdf:pdf},
	Isbn = {978-1-4244-1379-9},
	Issn = {1098-7576},
	Journal = {2007 International Joint Conference on Neural Networks},
	Month = {aug},
	Pages = {2734--2739},
	Publisher = {IEEE},
	Title = {{Dimensionality Reduction and Attack Recognition using Neural Network Approaches}},
	Url = {http://ieeexplore.ieee.org/document/4371391/ http://ieeexplore.ieee.org/lpdocs/epic03/
wrapper.htm?arnumber=4371391},
	Year = {2007},
	Bdsk-Url-1 = {http://ieeexplore.ieee.org/document/4371391/%20http://ieeexplore.ieee.org/lpdocs/
epic03/wrapper.htm?arnumber=4371391},
	Bdsk-Url-2 = {http://dx.doi.org/10.1109/IJCNN.2007.4371391}}

@article{Hansman2005,
	Abstract = {Attacks over the years have become both increasingly numerous and sophisticated. This
paper focuses on the provisioning of a method for the analysis and categorisation of both computer and
network attacks, thus providing assistance in combating new attacks, improving computer and network
security as well as providing consistency in language when describing attacks. Such a taxonomy is designed
to be useful to information bodies such as CERTs (Computer Emergency Response Teams) who have to
handle and categorise an every increasing number of attacks on a daily basis. Information bodies could use
the taxonomy to communicate more effectively as the taxonomy would provide a common classification
scheme. The proposed taxonomy consists of four dimensions which provide a holistic taxonomy in order to
deal with inherent problems in the computer and network attack field. The first dimension covers the attack
vector and the main behaviour of the attack. The second dimension allows for classification of the attack
targets. Vulnerabilities are classified in the third dimension and payloads in the fourth. Finally, to demonstrate
the usefulness of this taxonomy, a case study applies the taxonomy to a number of well known attacks. ??
2005 Elsevier Ltd. All rights reserved.},
	Annote = {NULL},
	Author = {Hansman, Simon and Hunt, Ray},
	Doi = {10.1016/j.cose.2004.06.011},
	File = {:Users/pooria/Downloads/f6faa55c4229d537b7f3377d15dfb91a8bfa.pdf:pdf},
	Isbn = {0167-4048},
	Issn = {01674048},
	Journal = {Computers and Security},
	Keywords = {Attack target,Attack vector,CERT,Classification scheme,Computer attack,Network
attack,Taxonomy},
	Number = {1},
	Pages = {31--43},
	Title = {{A taxonomy of network and computer attacks}},
	Volume = {24},
	Year = {2005},
	Bdsk-Url-1 = {http://dx.doi.org/10.1016/j.cose.2004.06.011}}

@article{Hawkins2002,
	Abstract = {We consider the problem of finding outliers in large multi- variate databases. Outlier detection can be applied during the data cleansing process of data mining to identify problems with the data itself, and to fraud detection where groups of outliers are often of particular interest.We use replicator neural networks (RNNs) to provide a measure of the outlyingness of data records. The performance of the RNNs is as- sessed using a ranked score measure. The effectiveness of the RNNs for outlier detection is demonstrated on two publicly available databases. 1},
	Annote = {NULL},
	Author = {Hawkins, Simon and He, Hongxing and Williams, Graham and Baxter, Rohan},
	Doi = {10.1007/978-3-540-74553-2},
	File = {:Users/pooria/Downloads/chp{\%}3A10.1007{\%}2F3-540-46145-0{\_}17.pdf:pdf},
	Isbn = {3540441239},
	Issn = {0302-9743},
	Journal = {Data Warehousing and {\ldots}},
	Pages = {170--180},
	Title = {{Outlier Detection Using Replicator Neural Networks}},
	Url = {http://link.springer.com/chapter/10.1007/3-540-46145-0{\_}17},
	Year = {2002},
	Bdsk-Url-1 = {http://link.springer.com/chapter/10.1007/3-540-46145-0%7B%5C_%7D17},
	Bdsk-Url-2 = {http://dx.doi.org/10.1007/978-3-540-74553-2}}

@article{Hodo2017,
	Abstract = {Intrusion detection has attracted a considerable interest from researchers and industries. The community, after many years of research, still faces the problem of building reliable and efficient IDS that are capable of handling large quantities of data, with changing patterns in real time situations. The work presented in this manuscript classifies intrusion detection systems (IDS). Moreover, a taxonomy and survey of shallow and deep networks intrusion detection systems is presented based on previous and current works. This taxonomy and survey reviews machine learning techniques and their performance in detecting anomalies. Feature selection which influences the effectiveness of machine learning (ML) IDS is discussed to explain the role of feature selection in the classification and training phase of ML IDS. Finally, a discussion of the false and true positive alarm rates is presented to help researchers model reliable and efficient machine learning based intrusion detection systems.},
	Annote = {76 ghorbani book
117
122
128
141 rnn (bull shit)
143 autoencoder (READ-bullshit)
144 rbm [one of the best]
146-147 DBN (under investigatio)
147: bullshit},
	Archiveprefix = {arXiv},
	Arxivid = {1701.02145},
	Author = {Hodo, Elike and Bellekens, Xavier and Hamilton, Andrew and Tachtatzis, Christos},
	Eprint = {1701.02145},
	File = {:Users/pooria/Library/Application Support/Mendeley Desktop/Downloaded/Hodo et al. - 2017 - Shallow and Deep Networks Intrusion Detection System A Taxonomy and Survey.pdf:pdf},
	Keywords = {alarm rates and true,deep networks,false positive,intrusion detection,positive alarm rates,shallow network},
	Month = {jan},
	Pages = {1--43},
	Title = {{Shallow and Deep Networks Intrusion Detection System : A Taxonomy and Survey}},
	Url = {http://arxiv.org/abs/1701.02145},
	Year = {2017},
	Bdsk-Url-1 = {http://arxiv.org/abs/1701.02145}}

@inproceedings{Javaid2016,
	Annote = {These guys already are using sparse autoencoder to capture the idea of feature learning ...
but why are they using it on NSL-KDD dataset? Isn't it a completely pointless if you are not going to be using
it on the raw dataset !},
	Author = {Javaid, Ahmad and Niyaz, Quamar and Sun, Weiqing and Alam, Mansoor},
	Booktitle = {Proceedings of the 9th EAI International Conference on Bio-inspired Information and
Communications Technologies (formerly BIONETICS)},
	Doi = {10.4108/eai.3-12-2015.2262516},
	File = {:Users/pooria/Library/Application Support/Mendeley Desktop/Downloaded/Javaid et al. - 2016 -
A Deep Learning Approach for Network Intrusion Detection System.pdf:pdf},
	Isbn = {978-1-63190-100-3},
	Keywords = {deep learning,network security,nids,nsl-kdd,sparse autoencoder},
	Pages = {21--26},
	Publisher = {ACM},
	Title = {{A Deep Learning Approach for Network Intrusion Detection System}},
	Url = {http://eudl.eu/doi/10.4108/eai.3-12-2015.2262516},
	Year = {2016},
	Bdsk-Url-1 = {http://eudl.eu/doi/10.4108/eai.3-12-2015.2262516},
	Bdsk-Url-2 = {http://dx.doi.org/10.4108/eai.3-12-2015.2262516}}

@article{Joseph2009,
	Annote = {[2,8,22] {\textless}{\~{}}{\~{}}{\~{}} some defensive techniques against adverserial machine
learning
and 4

[31-26] {\textless}{\~{}}{\~{}}{\~{}} red herring

[28] {\textless}{\~{}}{\~{}}{\~{}} PCA sensitivity},
	Author = {Joseph, Anthony D and Taft, Nina},
	File = {:Users/pooria/Downloads/rpca{\_}imc09.pdf:pdf},
	Isbn = {9781605587707},
	Journal = {Traffic},
	Keywords = {adversarial learning,network traffic analysis,principal components analysis,robust
statistics},
	Number = {November},
	Pages = {1--14},
	Title = {{ANTIDOTE : Understanding and Defending against}},
	Year = {2009}}

@article{Joshi2005,
	Abstract = {Hidden Markov Model (HMM) based applications are common in various areas, but the
incorporation of HMM's for anomaly detection is still in its infancy. This paper aims at classifying the TCP
network traffic as an attack or normal using HMM. The paper's main objective is to build an anomaly
detection system, a predictive model capable of discriminating between normal and abnormal behavior of
network traffic. In the training phase, special attention is given to the initialization and model selection issues,
which makes the training phase particularly effective. For training HMM, 12.195{\%} features out of the total
features (5 features out of 41 features) present in the KDD Cup 1999 data set are used. Result of tests on
the KDD Cup 1999 data set shows that the proposed system is able to classify network traffic in proportion to
the number of features used for training HMM. We are extending our work on a larger data set for building an
anomaly detection system.},
	Annote = {Bullshit paper ... they are assuming that each feature, can be considered a sequence !
WTF !},
	Author = {Joshi, Shrijit S and Phoha, Vir V},
	Doi = {10.1145/1167350.1167387},
	File = {:Users/pooria/Downloads/p98-joshi.pdf:pdf},
	Isbn = {1595930590},
	Journal = {Proceedings of the 43rd annual southeast regional conference on - ACM-SE 43},
	Keywords = {anomaly detection system,hidden markov models},
	Pages = {98},
	Title = {{Investigating hidden Markov models capabilities in anomaly detection}},
	Url = {http://portal.acm.org/citation.cfm?doid=1167350.1167387},
	Volume = {1},
	Year = {2005},
	Bdsk-Url-1 = {http://portal.acm.org/citation.cfm?doid=1167350.1167387},
	Bdsk-Url-2 = {http://dx.doi.org/10.1145/1167350.1167387}}

@article{Kamyshanska2013,
	Abstract = {Autoencoders are popular feature learning models because they are conceptually simple,
easy to train and allow for efficient inference and training. Recent work has shown how certain autoencoders
can assign an unnormalized "score" to data which measures how well the autoencoder can represent the
data. Scores are commonly computed by using training criteria that relate the autoencoder to a probabilistic
model, such as the Restricted Boltzmann Machine. In this paper we show how an autoencoder can assign
meaningful scores to data independently of training procedure and without reference to any probabilistic
model, by interpreting it as a dynamical system. We discuss how, and under which conditions, running the
dynamical system can be viewed as performing gradient descent in an energy function, which in turn allows
us to derive a score via integration. We also show how one can combine multiple, unnormalized scores into
a generative classifier. Copyright 2013 by the author(s).},
	Annote = {NULL},
	Author = {Kamyshanska, Hanna and Memisevic, Roland},
	File = {:Users/pooria/Downloads/kamyshanska13.pdf:pdf},
	Journal = {Proceedings of The 30th International Conference on Machine Learning},
	Keywords = {Dynamical systems,Learning systems},
	Pages = {1757--1765},
	Title = {{On autoencoder scoring}},
	Url = {http://jmlr.org/proceedings/papers/v28/kamyshanska13.pdf},
	Volume = {28},
	Year = {2013},
	Bdsk-Url-1 = {http://jmlr.org/proceedings/papers/v28/kamyshanska13.pdf}}

@article{Kandhari2009,
	Abstract = {Anomaly detection is an important problem that has been researched within diverse
research areas and application domains.Many anomaly detection techniques have been specifically
developed for certain appli- cation domains, while others are more generic. This survey tries to provide a
structured and comprehensive overview of the research on anomaly detection.We have grouped existing
techniques into different categories based on the underlying approach adopted by each technique. For each
category we have identified key as- sumptions, which are used by the techniques to differentiate between
normal and anomalous behavior.When applying a given technique to a particular domain, these assumptions
can be used as guidelines to assess the effectiveness of the technique in that domain. For each category, we
provide a basic anomaly detection technique, and then show how the different existing techniques in that
category are variants of the basic technique. This template provides an easier and more succinct
understanding of the techniques belonging to each category. Further, for each category, we identify the
advantages and disadvantages of the techniques in that category.We also provide a discussion on the
computational complexity of the techniques since it is an important issue in real application domains. We
hope that this survey will provide a better understanding of the different directions in which research has
been done on this topic, and how techniques developed in one area can be applied in domains for which they were not intended to begin with},
	Annote = {NULL},
	Archiveprefix = {arXiv},
	Arxivid = {arXiv:1011.1669v3},
	Author = {Kandhari, Rupali and Chandola, Varun and Banerjee, Arindam and Kumar, Vipin and Kandhari, Rupali},
	Doi = {10.1145/1541880.1541882},
	Eprint = {arXiv:1011.1669v3},
	File = {:Users/pooria/Library/Application Support/Mendeley Desktop/Downloaded/Chandola, Banerjee, Kumar - 2009 - Anomaly detection(2).pdf:pdf},
	Isbn = {0818663359},
	Issn = {03600300},
	Journal = {ACM Computing Surveys},
	Keywords = {Anomaly detection,outlier detection},
	Month = {jul},
	Number = {3},
	Pages = {1--6},
	Pmid = {21834704},
	Publisher = {ACM},
	Title = {{Anomaly detection}},
	Url = {http://portal.acm.org/citation.cfm?doid=1541880.1541882},
	Volume = {41},
	Year = {2009},
	Bdsk-Url-1 = {http://portal.acm.org/citation.cfm?doid=1541880.1541882},
	Bdsk-Url-2 = {http://dx.doi.org/10.1145/1541880.1541882}}

@article{Kantchelian2013,
	Abstract = {In this position paper, we argue that to be of practical interest, a machine-learning based security system must engage with the human operators beyond feature engineering and instance labeling to address the challenge of drift in adversarial environments. We propose that designers of such systems broaden the classification goal into an explanatory goal, which would deepen the interaction with system's operators.$\backslash$r$\backslash$nTo provide guidance, we advocate for an approach based on maintaining one classifier for each class of unwanted activity to be filtered. We also emphasize the necessity for the system to be responsive to the operators constant curation of the training set. We show how this paradigm provides a property we call isolation and how it relates to classical causative attacks.$\backslash$r$\backslash$nIn order to demonstrate the effects of drift on a binary classification task, we also report on two experiments using a previously unpublished malware data set where each instance is timestamped$\backslash$r$\backslash$naccording to when it was seen.},
	Annote = {45 IDS semantic gap
Read 8: it is a robust anomoly model against "poisining attack"

Read 37,21: both for detecting drift},
	Author = {Kantchelian, Alex and Afroz, Sadia and Huang, Ling and Islam, Aylin Caliskan and Miller, Brad and Tschantz, Michael Carl and Greenstadt, Rachel and Joseph, Anthony D and Tygar, J.D.},
	Doi = {10.1145/2517312.2517320},
	File = {:Users/pooria/Downloads/aisec08-kantchelian.pdf:pdf},
	Isbn = {9781450324885},
	Issn = {15437221},
	Journal = {AISec},
	Keywords = {D46 [Security and Pro-tection],H12 [User/Machine Systems],Invasive software,Learning,concept drift,malware classification},
	Pages = {99--109},
	Title = {{Approaches to Adversarial Drift}},
```

Year = {2013},
Bdsk-Url-1 = {http://dx.doi.org/10.1145/2517312.2517320}}

@inproceedings{Kim2016,
Abstract = {Due to the advance of information and communication techniques, sharing information through online has been increased. And this leads to creating the new added value. As a result, various online services were created. However, as increasing connection points to the internet, the threats of cyber security have also been increasing. Intrusion detection system(IDS) is one of the important security issues today. In this paper, we construct an IDS model with deep learning approach. We apply Long Short Term Memory(LSTM) architecture to a Recurrent Neural Network(RNN) and train the IDS model using KDD Cup 1999 dataset. Through the performance test, we confirm that the deep learning approach is effective for IDS.},
Author = {Kim, Jaehyun Jihyun and Kim, Jaehyun Jihyun and Thu, Huong Le Thi and Kim, Howon},
Booktitle = {2016 International Conference on Platform Technology and Service (PlatCon)},
Doi = {10.1109/PlatCon.2016.7456805},
File = {:Users/pooria/Downloads/07456805.pdf:pdf},
Isbn = {978-1-4673-8685-2},
Keywords = {Computer architecture,IDS model,Internet,Intrusion detection,KDD Cup 1999 dataset,LSTM RNN classifier,Logic gates,Mathematical model,Microprocessors,Recurrent neural networks,cyber security,deep learning,intrusion detection system,long short term memory architecture,neural net architecture,pattern classification,recurrent neural nets,recurrent neural network,security of data},
Month = {feb},
Pages = {1--5},
Publisher = {IEEE},
Title = {{Long Short Term Memory Recurrent Neural Network Classifier for Intrusion Detection}},
Url = {http://ieeexplore.ieee.org/document/7456805/ http://ieeexplore.ieee.org/document/7456805/{\%}5Cnhttp://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=7456805},
Year = {2016},
Bdsk-Url-1 = {http://dx.doi.org/10.1109/PlatCon.2016.7456805}}

@article{Lakhina2004,
Abstract = {Detecting and understanding anomalies in IP networks is an open and ill-defined problem. Toward this end, we have recently proposed the subspace method for anomaly diagnosis. In this paper we present the first large-scale exploration of the power of the subspace method when applied to flow traffic. An important aspect of this approach is that it fuses information from flow measurements taken throughout a network. We apply the subspace method to three different types of sampled flow traffic in a large academic network: multivariate timeseries of byte counts, packet counts, and IP-flow counts. We show that each traffic type brings into focus a different set of anomalies via the subspace method. We illustrate and classify the set of anomalies detected. We find that almost all of the anomalies detected represent events of interest to network operators. Furthermore, the anomalies span a remarkably wide spectrum of event types, including denial of service attacks (single-source and distributed), flash crowds, port scanning, downstream traffic engineering, high-rate flows, worm propagation, and network outage.},
Author = {Lakhina, Anukool and Crovella, Mark and Diot, Christiphe},
Doi = {10.1145/1028788.1028813},
File = {:Users/pooria/Library/Application Support/Mendeley Desktop/Downloaded/Lakhina, Crovella, Diot - 2004 - Characterization of Network-Wide Anomalies in Traffic Flows.pdf:pdf},
Isbn = {1581138210},
Issn = {00283940},
Journal = {Proceedings of the 4th ACM SIGCOMM conference on Internet measurement - IMC '04},
Keywords = {anomaly detection,ccr-0325701,crovella was,grants ani-9986397 and,in part by nsf,network traffic analysis,this work was performed,this work was supported,while m},
Pages = {201},
Pmid = {9689627},
Title = {{Characterization of network-wide anomalies in traffic flows}},

```
	Url = {http://portal.acm.org/citation.cfm?doid=1028788.1028813},
	Volume = {6},
	Year = {2004},
	Bdsk-Url-1 = {http://portal.acm.org/citation.cfm?doid=1028788.1028813},
	Bdsk-Url-2 = {http://dx.doi.org/10.1145/1028788.1028813}}

@article{Lakhina2004a,
	Abstract = {Anomalies are unusual and significant changes in a network's traffic levels, which can often span multiple links. Diagnosing anomalies is critical for both network operators and end users. It is a difficult problem because one must extract and interpret anomalous patterns from large amounts of high-dimensional, noisy data.In this paper we propose a general method to diagnose anomalies. This method is based on a separation of the high-dimensional space occupied by a set of network traffic measurements into disjoint subspaces corresponding to normal and anomalous network conditions. We show that this separation can be performed effectively by Principal Component Analysis.Using only simple traffic measurements from links, we study volume anomalies and show that the method can: (1) accurately detect when a volume anomaly is occurring; (2) correctly identify the underlying origin-destination (OD) flow which is the source of the anomaly; and (3) accurately estimate the amount of traffic involved in the anomalous OD flow.We evaluate the method's ability to diagnose (i.e., detect, identify, and quantify) both existing and synthetically injected volume anomalies in real traffic from two backbone networks. Our method consistently diagnoses the largest volume anomalies, and does so with a very low false alarm rate.},
	Annote = {NULL},
	Author = {Lakhina, Anukool and Crovella, Mark and Diot, Christophe},
	Doi = {10.1145/1030194.1015492},
	File = {:Users/pooria/Downloads/p219-lakhina.pdf:pdf},
	Isbn = {1581138628},
	Issn = {01464833},
	Journal = {ACM SIGCOMM Computer Communication Review},
	Keywords = {anomaly detection,network traffic analysis},
	Number = {4},
	Pages = {219},
	Pmid = {9689626},
	Title = {{Diagnosing network-wide traffic anomalies}},
	Url = {http://dl.acm.org/citation.cfm?id=1030194.1015492},
	Volume = {34},
	Year = {2004},
	Bdsk-Url-1 = {http://dl.acm.org/citation.cfm?id=1030194.1015492},
	Bdsk-Url-2 = {http://dx.doi.org/10.1145/1030194.1015492}}

@article{Lakhina2005,
	Abstract = {The increasing practicality of large-scale flow capture makes it possible to conceive of traffic analysis methods that detect and identify a large and diverse set of anomalies. However the challenge of effectively analyzing this massive data source for anomaly diagnosis is as yet unmet. We argue that the distributions of packet features (IP addresses and ports) observed in flow traces reveals both the presence and the structure of a wide range of anomalies. Using entropy as a summarization tool, we show that the analysis of feature distributions leads to significant advances on two fronts: (1) it enables highly sensitive detection of a wide range of anomalies, augmenting detections by volume-based methods, and (2) it enables automatic classification of anomalies via unsupervised learning. We show that using feature distributions, anomalies naturally fall into distinct and meaningful clusters. These clusters can be used to automatically classify anomalies and to uncover new anomaly types. We validate our claims on data from two backbone networks (Abilene and Geant) and conclude that feature distributions show promise as a key element of a fairly general network anomaly diagnosis framework.},
	Annote = {This guy uses PCA
topK components and k-topK to decompose a vector X
X = x1 + x2 where x1 is projection on topK and x2 is projection on k-topK , and the IIx2II gives you the
```

```
degree of anamoly !},
	Author = {Lakhina, Anukool and Crovella, Mark and Diot, Christophe},
	Doi = {10.1145/1090191.1080118},
	File = {:Users/pooria/Library/Application Support/Mendeley Desktop/Downloaded/Lakhina, Crovella,
Diot - Unknown - Mining Anomalies Using Traffic Feature Distributions.pdf:pdf},
	Isbn = {1595930094},
	Issn = {01464833},
	Journal = {ACM SIGCOMM Computer Communication Review},
	Keywords = {anomaly classification,anomaly detection,network-wide traf-},
	Number = {4},
	Pages = {217},
	Title = {{Mining anomalies using traffic feature distributions}},
	Volume = {35},
	Year = {2005},
	Bdsk-Url-1 = {http://dx.doi.org/10.1145/1090191.1080118}}

@article{Lakhina2004b,
	Abstract = {Network traffic arises from the superposition of Origin-Destination (OD) flows. Hence, a
thorough understanding of OD flows is essential for modeling network traffic, and for addressing a wide
variety of problems including traffic engineering, traffic matrix estimation, capacity planning, forecasting and
anomaly detection. However, to date, OD flows have not been closely studied, and there is very little known
about their properties.We present the first analysis of complete sets of OD flow time-series, taken from two
different backbone networks (Abilene and Sprint-Europe). Using Principal Component Analysis (PCA), we
find that the set of OD flows has small intrinsic dimension. In fact, even in a network with over a hundred OD
flows, these flows can be accurately modeled in time using a small number (10 or less) of independent
components or dimensions.We also show how to use PCA to systematically decompose the structure of OD
flow timeseries into three main constituents: common periodic trends, short-lived bursts, and noise. We
provide insight into how the various constitutents contribute to the overall structure of OD flows and explore
the extent to which this decomposition varies over time.},
	Author = {Lakhina, Anukool and Papagiannaki, Konstantina and Crovella, Mark and Diot, Christophe
and Kolaczyk, Eric D and Taft, Nina},
	Doi = {10.1145/1012888.1005697},
	File = {:Users/pooria/Library/Application Support/Mendeley Desktop/Downloaded/Lakhina et al. -
Unknown - Structural Analysis of Network Traffic Flows.pdf:pdf},
	Isbn = {1581138733},
	Issn = {01635999},
	Journal = {ACM SIGMETRICS Performance Evaluation Review},
	Keywords = {C43 [Performance of Systems],Modeling Techniques General Terms
Measurement,Network Opera-tions,Performance Keywords Network Traffic Analysis,Principal Compo-nent
Analysis,Traffic Engineering},
	Number = {1},
	Pages = {61},
	Title = {{Structural analysis of network traffic flows}},
	Volume = {32},
	Year = {2004},
	Bdsk-Url-1 = {http://dx.doi.org/10.1145/1012888.1005697}}

@article{Liao2013,
	Abstract = {With the increasing amount of network throughput and security threat, the study of intrusion
detection systems (IDSs) has received a lot of attention throughout the computer science field. Current IDSs
pose challenges on not only capricious intrusion categories, but also huge computational power. Though
there is a number of existing literatures to IDS issues, we attempt to give a more elaborate image for a
comprehensive review. Through the extensive survey and sophisticated organization, we propose the
taxonomy to outline modern IDSs. In addition, tables and figures we summarized in the content contribute to
```

```
easily grasp the overall picture of IDSs.},
	Annote = {NULL},
	Archiveprefix = {arXiv},
	Arxivid = {arXiv:1401.1637v1},
	Author = {Liao, Hung-Jen and {Richard Lin}, Chun-Hung and Lin, Ying-Chih and Tung, Kuang-Yuan},
	Doi = {10.1016/j.jnca.2012.09.004},
	Eprint = {arXiv:1401.1637v1},
	File = {:Users/pooria/Library/Application Support/Mendeley Desktop/Downloaded/Liao et al. - 2013 - Intrusion detection system A comprehensive review.pdf:pdf},
	Isbn = {1084-8045},
	Issn = {10848045},
	Journal = {Journal of Network and Computer Applications},
	Keywords = {Anomaly,Intrusion detection,Misuse},
	Number = {1},
	Pages = {16--24},
	Pmid = {17859689},
	Title = {{Intrusion detection system: A comprehensive review}},
	Url = {http://www.sciencedirect.com/science/article/pii/S1084804512001944},
	Volume = {36},
	Year = {2013},
	Bdsk-Url-1 = {http://www.sciencedirect.com/science/article/pii/S1084804512001944},
	Bdsk-Url-2 = {http://dx.doi.org/10.1016/j.jnca.2012.09.004}}

@inproceedings{Ma2013,
	Abstract = {Detecting outliers from big data plays an important role in network security. Previous outlier detection algorithms are generally incapable of handling big data. In this paper we present an parallel outlier detection method for big data, based on a new parallel auto-encoder method. Specifically, we build a replicator model of the input data to obtain the representation of sample data. Then, the replicator model is used to measure the replicability of test data, where records having higher reconstruction errors are classified as outliers. Experimental results show the performance of the proposed parallel algorithm. {\^{A}}{\textcopyright} 2013 IEEE.},
	Annote = {NULL},
	Author = {Ma, Yunlong and Zhang, Peng and Cao, Yanan and Guo, Li},
	Booktitle = {Proceedings - 2013 IEEE International Conference on Big Data, Big Data 2013},
	Doi = {10.1109/BigData.2013.6691791},
	File = {:Users/pooria/Downloads/06691791.pdf:pdf},
	Isbn = {9781479912926},
	Keywords = {Map-Reduce,outlier detection,parallel auto-encoder,replicator neural network},
	Number = {3},
	Pages = {15--17},
	Title = {{Parallel auto-encoder for efficient outlier detection}},
	Volume = {2},
	Year = {2013},
	Bdsk-Url-1 = {http://dx.doi.org/10.1109/BigData.2013.6691791}}

@article{McHugh2000,
	Abstract = {In 1998 and again in 1999, the Lincoln Laboratory of MIT conducted a comparative evaluation of intrusion detection systems (IDSs) developed under DARPA funding. While this evaluation represents a significant and monumental undertaking, there are a number of issues associated with its design and execution that remain unsettled. Some methodologies used in the evaluation are questionable and may have biased its results. One problem is that the evaluators have published relatively little concerning some of the more critical aspects of their work, such as validation of their test data. The appropriateness of the evaluation techniques used needs further investigation. The purpose of this article is to attempt to identify the shortcomings of the Lincoln Lab effort in the hope that future efforts of this kind will
```

be placed on a sounder footing. Some of the problems that the article points out might well be resolved if the evaluators were to publish a detailed description of their procedures and the rationale thatled to their adoption, but other problems would clearly remain.},
Author = {McHugh, John},
Doi = {10.1145/382912.382923},
File = {:Users/pooria/Library/Application Support/Mendeley Desktop/Downloaded/Hugh - Unknown - Testing Intrusion Detection Systems A Critique of the 1998 and 1999 DARPA Intrusion Detection System Evaluations as Per.pdf:pdf},
Isbn = {1094-9224},
Issn = {10949224},
Journal = {ACM Transactions on Information and System Security},
Keywords = {Categories and Subject Descriptors,Computer security,Security Additional Key Words and Phrases,Security and Protection---Invasive software (eg,Trojan horses) General Terms,intrusion detection,receiver operating curves (ROC),software evaluation,viruses,worms},
Number = {4},
Pages = {262--294},
Title = {{Testing Intrusion detection systems: a critique of the 1998 and 1999 DARPA intrusion detection system evaluations as performed by Lincoln Laboratory}},
Volume = {3},
Year = {2000},
Bdsk-Url-1 = {http://dx.doi.org/10.1145/382912.382923}}

@article{Ringberg2007,
Abstract = {Detecting anomalous traffic is a crucial part of managing IP networks. In recent years, network-wide anomaly detection based on Principal Component Analysis (PCA) has emerged as a powerful method for detecting a wide variety of anomalies. We show that tuning PCA to operate effectively in practice is difficult and requires more robust techniques than have been presented thus far. We analyze a week of network-wide traffic measurements from two IP backbones (Abilene and Geant) across three different traffic aggregations (ingress routers, OD flows, and input links), and conduct a detailed inspection of the feature time series for each suspected anomaly. Our study identifies and evaluates four main challenges of using PCA to detect traffic anomalies: (i) the false positive rate is very sensitive to small differences in the number of principal components in the normal subspace, (ii) the effectiveness of PCA is sensitive to the level of aggregation of the traffic measurements, (iii) a large anomaly may in advertently pollute the normal subspace, (iv) correctly identifying which flow triggered the anomaly detector is an inherently challenging problem. {\textcopyright} Copyright 2007 ACM.},
Annote = {Awesome paper to define short comings of PCA in "Traffic Anomaly Detection"

It has some analysis that measure the effectiveness of PCA.

This is the paper that gave me the idea of compare sensitivity of PCA and AE in terms of parameters

Two great papers to be read as well},
Author = {Ringberg, Haakon and Soule, Augustin and Rexford, Jennifer and Diot, Christophe},
Doi = {10.1145/1269899.1254895},
File = {:Users/pooria/Library/Application Support/Mendeley Desktop/Downloaded/Ringberg et al. - Unknown - Sensitivity of PCA for Traffic Anomaly Detection.pdf:pdf},
Isbn = {1595936394},
Issn = {01635999},
Journal = {ACM SIGMETRICS Performance Evaluation Review},
Keywords = {network traffic analysis,principal component analysis},
Number = {1},
Pages = {109},
Title = {{Sensitivity of PCA for traffic anomaly detection}},
Volume = {35},

```
	Year = {2007},
	Bdsk-Url-1 = {http://dx.doi.org/10.1145/1269899.1254895}}

@article{Rubinstein2008,
	Annote = {read [2] method for adding synthetic anomalies !},
	Author = {Rubinstein, BIP and Nelson, B and Huang, L and Joseph, A.D. and Lau, S. and Taft, Nina and
Tygar, JD},
	File = {:Users/pooria/Downloads/EECS-2008-73.pdf:pdf},
	Journal = {EECS Department, University of California, Berkeley, Tech. Rep. UCB/EECS-2008-73, May},
	Pages = {2008--73},
	Title = {{Compromising PCA-based anomaly detectors for network-wide traffic}},
	Url = {http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.158.5231{\&}rep=rep1{\&}type=pdf},
	Year = {2008},
	Bdsk-Url-1 = {http://citeseerx.ist.psu.edu/viewdoc/download?
doi=10.1.1.158.5231%7B%5C&%7Drep=rep1%7B%5C&%7Dtype=pdf}}

@article{Salama2011,
	Author = {Salama, Ma and Eid, Hf and Ramadan, Ra},
	Doi = {10.1007/978-3-642-20505-7_26},
	File = {:Users/pooria/Library/Application Support/Mendeley Desktop/Downloaded/Salama et al. - 2011 -
Hybrid Intelligent Intrusion Detection Scheme.pdf:pdf},
	Isbn = {9783642205040},
	Issn = {18675662},
	Journal = {Advances in Intelligent and Soft Computing},
	Pages = {293--303},
	Publisher = {Springer, Berlin, Heidelberg},
	Title = {{Hybrid intelligent intrusion detection scheme}},
	Url = {http://link.springer.com/10.1007/978-3-642-20505-7{\_}26 http://link.springer.com/chapter/
10.1007/978-3-642-20505-7{\_}26},
	Year = {2011},
	Bdsk-Url-1 = {http://link.springer.com/10.1007/978-3-642-20505-7%7B%5C_%7D26%20http://
link.springer.com/chapter/10.1007/978-3-642-20505-7%7B%5C_%7D26},
	Bdsk-Url-2 = {http://dx.doi.org/10.1007/978-3-642-20505-7_26}}

@article{Shyu2003,
	Abstract = {This paper proposes a novel scheme that uses robust principal component classifier in
intrusion detection problems where the training data may be unsupervised. Assuming that anomalies can be
treated as outliers, an intrusion predictive model is constructed from the major and minor principal
components of the normal instances. A measure of the difference of an anomaly from the normal instance is
the distance in the principal component space. The distance based on the major components that account
for 50{\%} of the total variation and the minor components whose eigenvalues less than 0.20 is shown to
work well. The experiments with KDD Cup 1999 data demonstrate that the proposed method achieves
98.94{\%} in recall and 97.89{\%} in precision with the false alarm rate 0.92{\%} and outperforms the nearest
neighbor method, density-based local outliers (LOF) approach, and the outlier detection algorithm based on
Canberra metric.},
	Author = {Shyu, Mei-ling and Chen, Shu-Ching and Sarinnapakorn, Kanoksri and Chang, Liwu},
	Doi = {10.1007/11539827-18},
	File = {:Users/pooria/Downloads/ADA465712.pdf:pdf},
	Isbn = {9783540283157},
	Issn = {1860949X},
	Journal = {Dtic},
	Keywords = {Anomaly detection,data mining,intrusion detection,outliers,principal component analysis},
	Number = {ADA465712},
	Title = {{A Novel Anomaly Detection Scheme Based on Principal Component Classifier}},
        Year = {2003},
        Bdsk-Url-1 = {http://dx.doi.org/10.1007/11539827-18}}

@inproceedings{Tavallaee2009,
        Abstract = {During the last decade, anomaly detection has attracted the attention of many researchers
to overcome the weakness of signature-based IDSs in detecting novel attacks, and KDDCUP'99 is the
mostly widely used data set for the evaluation of these systems. Having conducted a statistical analysis on
this data set, we found two important issues which highly affects the performance of evaluated systems, and
results in a very poor evaluation of anomaly detection approaches. To solve these issues, we have proposed
a new data set, NSL-KDD, which consists of selected records of the complete KDD data set and does not
suffer from any of mentioned shortcomings.},
        Archiveprefix = {arXiv},
        Arxivid = {arXiv:1011.1669v3},
        Author = {Tavallaee, Mahbod and Bagheri, Ebrahim and Lu, Wei and Ghorbani, Ali A},
        Booktitle = {IEEE Symposium on Computational Intelligence for Security and Defense Applications,
CISDA 2009},
        Doi = {10.1109/CISDA.2009.5356528},
        Eprint = {arXiv:1011.1669v3},
        File = {:Users/pooria/Library/Application Support/Mendeley Desktop/Downloaded/Tavallaee et al. -
Unknown - A Detailed Analysis of the KDD CUP 99 Data Set.pdf:pdf},
        Isbn = {9781424437641},
        Issn = {2329-6267},
        Pmid = {25246403},
        Title = {{A detailed analysis of the KDD CUP 99 data set}},
        Year = {2009},
        Bdsk-Url-1 = {http://dx.doi.org/10.1109/CISDA.2009.5356528}}

@article{Vasilomanolakis2015,
        Abstract = {The dependency of our society on networked computers has become frightening: In the
economy, all-digital networks have turned from facilitators to drivers; as cyber-physical systems are coming
of age, computer networks are now becoming the central nervous systems of our physical world-even of
highly critical infrastructures such as the power grid. At the same time, the 24/7 availability and correct
functioning of networked computers has become much more threatened: The number of sophisticated and
highly tailored attacks on IT systems has significantly increased. Intrusion Detection Systems (IDSs) are a
key component of the corresponding defense measures; they have been extensively studied and utilized in
the past. Since conventional IDSs are not scalable to big company networks and beyond, nor to massively
parallel attacks, Collaborative IDSs (CIDSs) have emerged. They consist of several monitoring components
that collect and exchange data. Depending on the specific CIDS architecture, central or distributed analysis
components mine the gathered data to identify attacks. Resulting alerts are correlated among multiple
monitors in order to create a holistic view of the network monitored. This article first determines relevant
requirements for CIDSs; it then differentiates distinct building blocks as a basis for introducing a CIDS design
space and for discussing it with respect to requirements. Based on this design space, attacks that evade
CIDSs and attacks on the availability of the CIDSs themselves are discussed. The entire framework of
requirements, building blocks, and attacks as introduced is then used for a comprehensive analysis of the
state of the art in collaborative intrusion detection, including a detailed survey and comparison of specific
CIDS approaches.},
        Author = {Vasilomanolakis, Emmanouil and Karuppayah, Shankar and Muehlhaeuser, Max and Fischer,
Mathias},
        Doi = {10.1145/2716260},
        File = {:Users/pooria/Library/Application Support/Mendeley Desktop/Downloaded/Vasilomanolakis et al.
- 2015 - Taxonomy and Survey of Collaborative Intrusion Detection(2).pdf:pdf},
        Isbn = {0360-0300},
        Issn = {15577341},
        Journal = {ACM Computing Surveys (CSUR)},
	Keywords = {Collaborative intrusion detection,attacks,classification,network security},
	Month = {may},
	Number = {4},
	Pages = {1--35},
	Publisher = {ACM},
	Title = {{Taxonomy and Survey of Collaborative Intrusion Detection}},
	Url = {http://dl.acm.org/citation.cfm?doid=2775083.2716260},
	Volume = {47},
	Year = {2015},
	Bdsk-Url-1 = {http://dl.acm.org/citation.cfm?doid=2775083.2716260},
	Bdsk-Url-2 = {http://dx.doi.org/10.1145/2716260}}

@article{Wang2015,
	Abstract = {Generally speaking, most systems of network traffic identification are based on features. The features may be port numbers, static signatures, statistic characteristics, and so on. The difficulty of the traffic identification is to find the features in the flow data. The process is very time-consuming. Also, these approaches are invalid to unknown protocol. To solve these problems, we propose a method that is based on neural network and deep learning -- a hotspot of research in machine learning. The results show that our approach works very well on the applications of feature learning, protocol identification and anomalous protocol detection.},
	Author = {Wang, Zhanyi},
	File = {:Users/pooria/Library/Application Support/Mendeley Desktop/Downloaded/Wang - Unknown - The Applications of Deep Learning on Traffic Identification.pdf:pdf},
	Journal = {Black Hat USA},
	Keywords = {anomalous protocol detection,deep learning,feature learning,protocol classification,traffic identification},
	Title = {{The Applications of Deep Learning on Traffic Identification}},
	Year = {2015}}

@article{Williams2002,
	Annote = {NULL},
	Author = {Williams, Graham and Gu, Lifang},
	File = {:Users/pooria/Desktop/01184035.pdf:pdf},
	Isbn = {0769517544},
	Pages = {709--712},
	Title = {{" for Outlier Detection in Data Mining}},
	Year = {2002}}
```