Paper 1: Active Learning From Imbalanced Data: A Solution of Online Weighted Extreme Learning Machine by Hualong Yu , Xibei Yang, Shang Zheng, and Changyin Sun

What problem does this paper try to solve, i.e., its motivation

Active Learning is a very advantageous tool to increasing the efficiency of machine learning applications. A problem that we encounter with active learning is that it runs into various issues when the input data is imbalanced and unevenly distributed. When this data is imbalanced, active learning models tend to skew and overfit based on whatever classifier is dominant. This leads to either low classification performance or high time consumption which are necessary problems to resolve.

How does it solve the problem?

The paper discusses their solution dubbed active online-weighted ELM(AOW-ELM) for pool-based batch-mode active learning based models. An ELM or extreme learning machine is a single feed forward neural network. This ELM is then weighted in order to resolve the issue of imbalanced classes. This is then combined with a designed weight updating model and an effective online-learning model to end up with their solution. This solution has comparable metrics in performance and accuracy to popular solutions such as SVM or MLP, and offers a significant time-save over earlier solutions to imbalanced datasets without a tradeoff to accuracy.

How the weighted ELM works is that it offers much larger penalty weights to the minority classes while providing much smaller penalties to larger classes. This allows the model to, in essence, balance it's predictions. The online learning aspect of this model allows for significant time complexity reductions due to taking data in as chunks.

A list of novelties/contributions

The paper spends time discussing why active learning is so affected by imbalanced data during training. The reason is very simple but interesting. In the interest of maximizing accuracy, it is much more accurate to lean towards misclassifying the minority class then misclassifying the majority class. Being correct on the majority of the data is better than being more correct on the minority of data. This obvious leads to overfitting and and a non generalizable model. The weighted ELM can resolve this by making the miss penalty less relevant for the desired classes which allows the classifier to work without inherent bias.

What do you think are the downsides of the work?

The experimental data was performed only on binary-class datasets. While not completely irrelevant, it is unclear how simple it would be to adapt this solution into datasets with more than two classes and how imbalances can be resolved with 3+ different sets. They do discuss that their next paper will focus on this topic though so this concern may be irrelevant soon. This is also only functionally tested on pool-based batch mode active learning model. As I am unfamiliar with how common these traits are in active learning situations, it remains a specialized solution for a specific job. While research in these areas is relevant and important to do nonetheless, there is not enough evidence of relevance to other aspects of active learning as a whole.

Paper 2: Supervised machine learning and active learning in classification of radiology reports | Journal of the American Medical Informatics Association | Oxford Academic

What problem does this paper try to solve, i.e., its motivation

The intention of this paper is to build a supervised machine learning model using active learning techniques to properly classify radiology reports. The goal is to create a model that is trained to detect whether a report contains a cancerous tumor or not. Given the high stakes of the situation, the model must be extremely sensitive, yet maintain a semblance of accuracy. It is much better to predict a false positive than a false negative in this case. Given the large amount of reports a cancer registry receives and the amount of negative cases, a machine learning model with significantly help with giving results back quickly and allow doctors to get ahead of possible medical emergencies.

How does it solve the problem?

ML models have been shown to be very accurate in determining cancer in radiology reports. Active Learning in this case can simply improve accuracy and training times without the need for lots of manually classified data. It also helps in the case where the majority of cases where nothing of relevance is present, and can bias more to looking for actual growths. This paper tests a variety of different AL models on datasets of cancers and compared them to each other to determine which performs the best. The models tested are Simple, Self-Confident (Self-Conf), Kernel Farthest-First (KFF), and Balanced Exploration and Exploitation (Balance-EE). The solution eventually agreed upon was the simple method, as there was no significant accuracy tradeoff as opposed to the simplicity of implementation.

A list of novelties/contributions

This research significantly contributes to the medical field. Doctors are notoriously overworked and providing them with a tool that can assist them in their job and allowing them to focus more effort in other aspects of their work is a fantastic things. Humans can get tired and make mistakes, while machines are consistent, even in their failures. Given the gravity of making an accurate and correct diagnosis, having two opinions on the matter will always be better than one.

What do you think are the downsides of the work?

As someone who has lots of family in medicine, there will always be a slight distrust in a model as opposed to a human eye. While this is maybe a moot point, it is difficult to convince some in the field to move forward with the adoption of new technologies.

There is always a concern with medical data being used in a machine learning model as it's very important to obfuscate any personally identifiable information. Given the data being used here, it's very difficult to gain any protected patient data that would be relevant. The nature of active learning would provide someone who is running this model the data of many different patients. Given an application of this solution in other medical fields, there may be concerns with the security and reversibility of the model.

Paper 3: Using active learning in intrusion detection | IEEE Conference Publication

What problem does this paper try to solve, i.e., its motivation

Intrusion detection systems or IDS's are used as a final security method in order to prevent any kind of third party interference or attack on a system. Usually, these systems must be continuously updated and are dependent on security experts to continuously update and improve systems. A machine learning model being trained with active learning may help with improving the two currently used methods. ISDs are often a combination of a misuse detection system which finds known attacks and a anomaly detection system which detects all oddities. The misuse detection fails at finding new types of attacks and the anomaly detection causes many false alarms. This is inefficient as is, and could be improved.

How does it solve the problem?

The paper proposes a combination of the two systems via an active learning model. A security expert trains an attack model and uses attack data to then train a model with this information to create a model that utilizes both the misuse and anomaly detection in conjunction to determine threats. It was found that this new active learning model was quite good at generating classifiers for different types of attacks. Using active learning allowed security experts to effectively teach the model to be more responsive to certain suspicious behaviors. Active learning also allows there to be less data for direct attacks and have the model still be responsive. As attacks are generally rare, the model must be good at detecting the difference between an attack and normal traffic despite it being a very slim minority.

The model in the paper uses SVM as the main classifier algorithm.

A list of novelties/contributions

Active Learning serves to reduce the amount of active work in labeling and preprocessing data for a model to be effective. Given that attacks are always evolving, having a machine learning model capable of responding and learning new attack behaviors is confidence inspiring. Using machine learning, especially active learning, in security based situations seems like a very useful application of the technology.

What do you think are the downsides of the work?

As mentioned in the paper, it's very difficult to find good attack data to train a security model on. Considering datasets from attack competitions like DEFCON can be unrepresentative of regular traffic considering that an attack would likely be a minority of all traffic. As is with all security algorithms and methods, it's very difficult to be ready for all cases which would require high sensitivity. High sensitivity in turn creates false alarms which are undesired and can lead to ignoring actual positives due to commonality. Also considering that these are often the last line of defense, it would be much more desired to have a specialized system capable of immediately detecting any anomalies even despite the difficulty of creatin one. This model may be better of as an early threat detection system rather than what it is currently.