Deep Learning Approach to Network Intrusion Detection

Paper By: Nathan Shone, Tran Nguyen Ngoc, Vu Dinh Phai, Qi Shi

Presented by: Romi Bajracharya
Overview

- Introduction
- Limitation with NIDS
- Proposed Model
- What is Deep Learning?
- Existing Framework
- Final Model
- Results
- Conclusion
Introduction

- Network Security has become one of the most important factors for companies to consider.
- Network Intrusion Detection System (NIDS), a device or software application that monitors a network or system to detect the malicious activity.
- NIDS plays crucial role in defending computer network.
- NIDS analyzes incoming network traffic to and from all the devices on the network.
- Once an attack is identified or if any abnormal activity is detected it will alert the administrator.
Limitations with NIDS

1. Drastic growth in the volume of network data. Dealing with these volumes requires techniques which can analyze data in an increasing rapid, efficient and effective manner. Estimated by 2020, the amount of data in existence will top 44ZB (Zeta Byte).

2. In-depth monitoring and granularity required to improve effectiveness and accuracy.

3. Even though in recent years machine learning mechanism was introduced. However, it required more human interaction, very expensive and was prone to error.

1 ZB = 1 Million Peta Byte
Proposed Model

- To overcome all those limitation, a new novel deep learning model to enable NIDS operation within Modern networks, i.e., Non-Symmetric Deep Auto Encoder (NDAE).
- Combination of deep and shallow learning, capable of correctly analyzing a wide range of network traffic.
- **Main goal**: Decrease the reliance on human operator, devise a technique capable of providing reliable unsupervised feature learning which can improve upon the performance and accuracy of existing technology.
- **Technology used**: GPU-enabled TensorFlow running on a 64-bit Ubuntu 16.04 with an Intel Xeon 3.60Ghz processor, 16GB RAM and an NVIDIA GTX 750 GPU
- **Dataset used**: KDD cup '99 (Knowledge Discover and Data mining)
- NSL-KDD (Network Security Library)
What is Deep Learning?

- It is a form of machine learning that enables to learn from experience
- The hierarchy of concepts allows the computer to learn complicated concepts by building them out of simpler ones
- Capable of automatically finding correlation in the data.
- Promising method of next generation of intrusion detection.
- Deep learning approach trains the artificial neural network to function as a biological neural network.
Existing technology (Encoder decoder Paradigm)

Single auto encoder

Stacked auto encoder
Methodology (NDAE)

- An auto encoder featuring non-symmetrical multiple hidden layers.
- Shifting from encoder decoder paradigm to encoder phase.
- Unlike a conventional auto encoder the proposed NDAE does not contain a decoder.
- Reduces computational time and overhead.
- Accuracy improves.
- Gives correct learning structure.

Typical auto encoder

Non-symmetric deep auto encoder (NDAE)
• Stacking NDAEs to create a deep learning hierarchy.
• Stacking NDAEs offer a layer wise unsupervised representation learning algorithm.
• Learn complex relationship between different features.
• RF algorithm groups “weak learner” to form a “strong leaner”.
• This models’ trains RF classifier using the encoded representation learned by the stacked NDAEs to classify network traffic into normal data and known attacks.
• Using this structure best results were obtained.
Accuracy Metrics (5 class performance)

- **Accuracy**: \( \frac{(TP+TN)}{(TP+TN+FP+FN)} \)
- **Precision**: \( \frac{TP}{(TP+FP)} \)
- **Recall**: \( \frac{TP}{(TP+FN)} \)
- **False Alarm**: \( \frac{FP}{(FP+TN)} \)
- **F-Score**: \( \frac{2 \times (\text{precision} \times \text{recall})}{(\text{Precision} + \text{Recall})} \)

1) **True Positive (TP)** - Attack data that is correctly classified as an attack.
2) **False Positive (FP)** - Normal data that is incorrectly classified as an attack.
3) **True Negative (TN)** - Normal data that is correctly classified as normal.
4) **False Negative (FN)** - Attack data that is incorrectly classified as normal.
5 Class performance comparison of Deep Beliefs Network (DBN) and Stacked Non-symmetric Deep Auto Encoder (S-NDAE) using KDD 99

<table>
<thead>
<tr>
<th>Attack Class</th>
<th>No. Training</th>
<th>No. Attacks</th>
<th>Accuracy (%)</th>
<th>Precision (%)</th>
<th>Recall (%)</th>
<th>F-Score (%)</th>
<th>False Alarm (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>DBN</td>
<td>S-NDAE</td>
<td>DBN</td>
<td>S-NDAE</td>
<td>DBN</td>
<td>S-NDAE</td>
<td>DBN</td>
</tr>
<tr>
<td>Normal</td>
<td>97278</td>
<td>60593</td>
<td>99.49</td>
<td>99.49</td>
<td>99.49</td>
<td>99.49</td>
<td>96.94</td>
</tr>
<tr>
<td>DoS</td>
<td>391458</td>
<td>223298</td>
<td>99.65</td>
<td>99.79</td>
<td>98.74</td>
<td>100.00</td>
<td>99.49</td>
</tr>
<tr>
<td>Probe</td>
<td>4107</td>
<td>2377</td>
<td>14.19</td>
<td>98.74</td>
<td>86.66</td>
<td>100.00</td>
<td>14.19</td>
</tr>
<tr>
<td>R2L</td>
<td>1126</td>
<td>5993</td>
<td>89.25</td>
<td>9.31</td>
<td>100.00</td>
<td>99.49</td>
<td>96.94</td>
</tr>
<tr>
<td>U2R</td>
<td>52</td>
<td>39</td>
<td>7.14</td>
<td>0.00</td>
<td>38.46</td>
<td>0.00</td>
<td>12.05</td>
</tr>
<tr>
<td>Total</td>
<td>494021</td>
<td>292300</td>
<td>97.90</td>
<td>97.85</td>
<td>97.81</td>
<td>99.99</td>
<td>97.47</td>
</tr>
</tbody>
</table>

**DoS**: Denial of Service  
**R2L**: Remote to User  
**U2R**: User to Root  
**Probe**: an attack which is deliberately crafted so that its target detects and reports it with a recognizable “fingerprint” in the report
Time comparison between DBN and S-NDAE using KDD data set

- NDAE approach of model
- Able to accomplish a significant reduction in required training time
- Conclusion: Using KDDs, this model maintains high levels of accuracy and decreases training time.

<table>
<thead>
<tr>
<th>No. Neurons in Hidden Layers</th>
<th>Training Time (s)</th>
<th>Time Saving (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>DBN</td>
<td>S-NDAE</td>
</tr>
<tr>
<td>8</td>
<td>54660</td>
<td>2024</td>
</tr>
<tr>
<td>14</td>
<td>122460</td>
<td>2381</td>
</tr>
<tr>
<td>22</td>
<td>204900</td>
<td>2446</td>
</tr>
</tbody>
</table>
5 Class performance comparison between DBN and S-NDAE using NSL-KDD

**DoS**: Denial of Service  
**R2L**: Remote to User  
**U2R**: User to Root  
**Probe**: an attack which is deliberately crafted so that its target detects and reports it with a recognizable “fingerprint” in the report
Time comparison between DBN and S-NDAE using NSL-KDD data set

<table>
<thead>
<tr>
<th>No. Neurons in Hidden Layers</th>
<th>Training Time (s) DBN</th>
<th>Time (s) S-NDAE</th>
<th>Time Saving (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>1198.08</td>
<td>644.84</td>
<td>46.18</td>
</tr>
<tr>
<td>14</td>
<td>10984.04</td>
<td>722.54</td>
<td>93.42</td>
</tr>
<tr>
<td>22</td>
<td>21731.76</td>
<td>1091.97</td>
<td>94.98</td>
</tr>
</tbody>
</table>
Conclusion

- Stacked NDAE model produced promising set of results.
- With KDD’99 dataset this model was able to offer an average accuracy of 97.85%.
- With NSL-KDD dataset, this model was able to offer an average accuracy of 85.42%.
- Lastly, although this model has managed to produce better results compared to models like DBN, this might not be the perfect solution and there is further room for improvement.