Pedrum Jalali

[Email address]

Network Intrusion Detection using The markov chain model

# Abstract

The purpose of this paper is to detect network intrusions using the markov chain model. The paper aims at targeting anomalies where there is a significant change in the pattern of connections made to a particular server. The data used in this paper is from the DARPA intrusion detection evaluation program in the year 1998.

# Traffic Sampling

During a 7 week period traffic coming in and out of a network system was monitored. Various controlled attacks where performed on the network at different times during the monitoring period. In this research we analyze the incoming connections to one of the servers.

# Theory

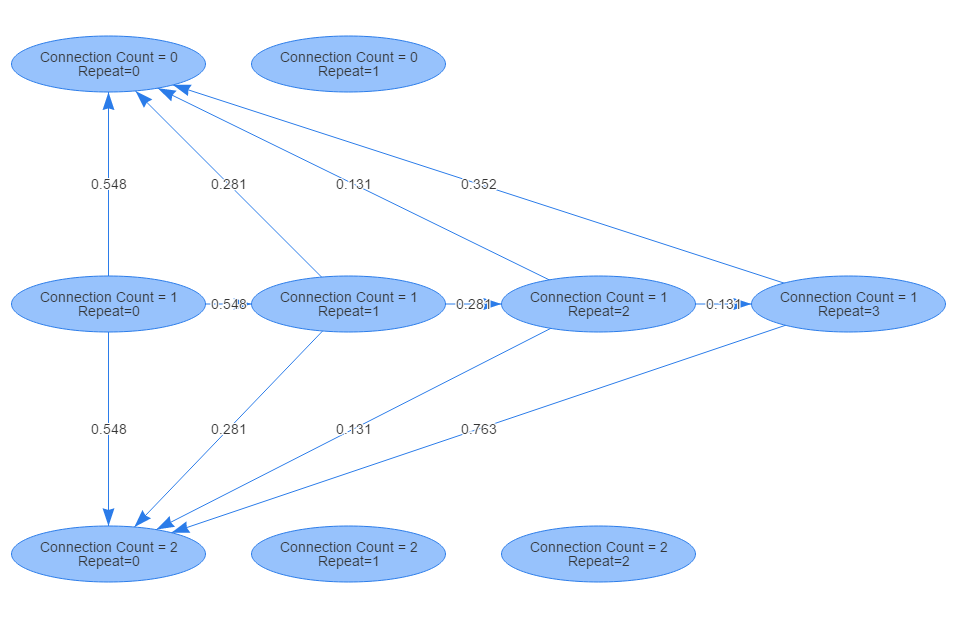
## Generating Clean Traffic Model

In the first stage of the research the clean traffics behavior was modeled using the markov chain model. The traffic was split into one minute periods. A state was defined using the properties below:

**Connection Count:** The number of connections that were initiated with the server during that one minute period.

**Repeat**: The number of previous intervals that the connection count property remained the same.

Each state has a series of actions. The actions show the probability that the state went from its current state to the next state. Therefore the markov chain model would look something like this. In order to avoid clutter in the figure below only the actions propagating from the states in the middle row have been drawn:



In order to explain the algorithm for determining the next state the following notation will be used:

The number of connections initiated with server during time interval i.

The number of consecutive times this connection count has been repeated up to interval i.

The state with connection count C and repeat R

The I’th one minute interval.

The algorithm for determining the next state is as follows:

**Step 1:** S = S(0, 0) and

**Step 2:**

**Step 3:** Find the number of connections initiated during.

If go to step 4.

If go to step 5.

**Step 4:** . Go to step 2.

**Step 5**:

**Step 6:**

## Generating The Probability Distribution

Once the markov chain model for the clean traffic has been generated, the following distribution probability is calculated:

Where:

The result of generating the probability distribution for the clean traffic are shown in the plots below. The 95% cutoff point can be obtained as follows:

0.000101

## Unfiltered Traffic Distribution:

Using the markov model for clean traffic, the unfiltered traffic was passed through the model and the distribution was calculated. The results have been plotted below. The large number of observations in the right most bucket was dues to observations with zero probability.

In the figure below the difference in log probability distribution between the 2 traffics is plotted below.. The really low and high end buckets have been removed for better visualization. It can be seen that the left hand buckets are positive which shows that clean traffic has a better correlation with the markov model. As we move to the left the values become negative indicating that the uncorrelation is more in the unfiltered traffic at that end.

## Attack Detection

In this paper our main goal was to find attacks where there is a significant change in incoming connections. Therefore our main targets where the following type of attacks:

* Network mapping
* Illegal upload of copyright content using Warez
* Illegal download of copyright content using Warez
* Syn flood denial of service
* Port sweep
* Network probing tools
* DOS attack using misfragmented UDP packets.
* DOS using ping of death

# Results

We considered Log(P)<-18 as our cutoff point for detecting attacks. The results are based on a 7 week period of monitoring:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | True Detections | False Alarms | Missed Attacks | Total Connections |
| Count | 20 | 7 | 4 | 25181 |
| Accuracy | 83% | 0.02% |  |  |

# References

*https://www.ll.mit.edu/ideval/data/1998data.html*. (1998).