

Application of Artificial Neural Networks in Detection of DOS Attacks

I. Ahmad, A. Abdullah, A. Alghamdi

International Conference on Security of Information and Networks, October 2009

Denial of Service Attacks

- Network is flooded with traffic.
- Saturates bandwidth capacity of target.
- Different methods of accomplishing a DOS attack:
 - Ping of Death
 - Smurf
 - Neptune

Network Intrusion Detection System

- Monitors network traffic to detect:
 - Anomalies: diff from established users
 - Misuse: similar to hacker behavior
 - Patterns: against DB of known patterns
- Challenge of IDS:
 - Have high detection rate
 - Have low false positive rate

Authors' Objective

- Create a neural network to detect DOS attacks.
- Network traffic would be input to NN
- Output would classify traffic as normal or abnormal.

Data Set

- Use Kddcup99 data set from DARPA.
- Created using simulated network traffic.
- Common network data set used by network researchers.
- Gives data close to real network data, without privacy concerns or loss of data through sanitization.

Determining NN Architecture

- Trained multiple network architectures using multiple activation functions.
- Compared the NNs through the root mean squared error.
- Settled on the architecture that had the smallest RMSE.
- Used the activation function with the highest detection rate.

Neural Network Architecture

- Feed-forward network with 2 hidden layers.
- Input layer: 41 neurons (one per field in data set)
- Hidden layer 1: 14 neurons
- Hidden layer 2: 9 neurons
- Output layer: 2 neurons (signifying normal packet vs abnormal packet)
- Created with Java Object Oriented Neural Network Engine.

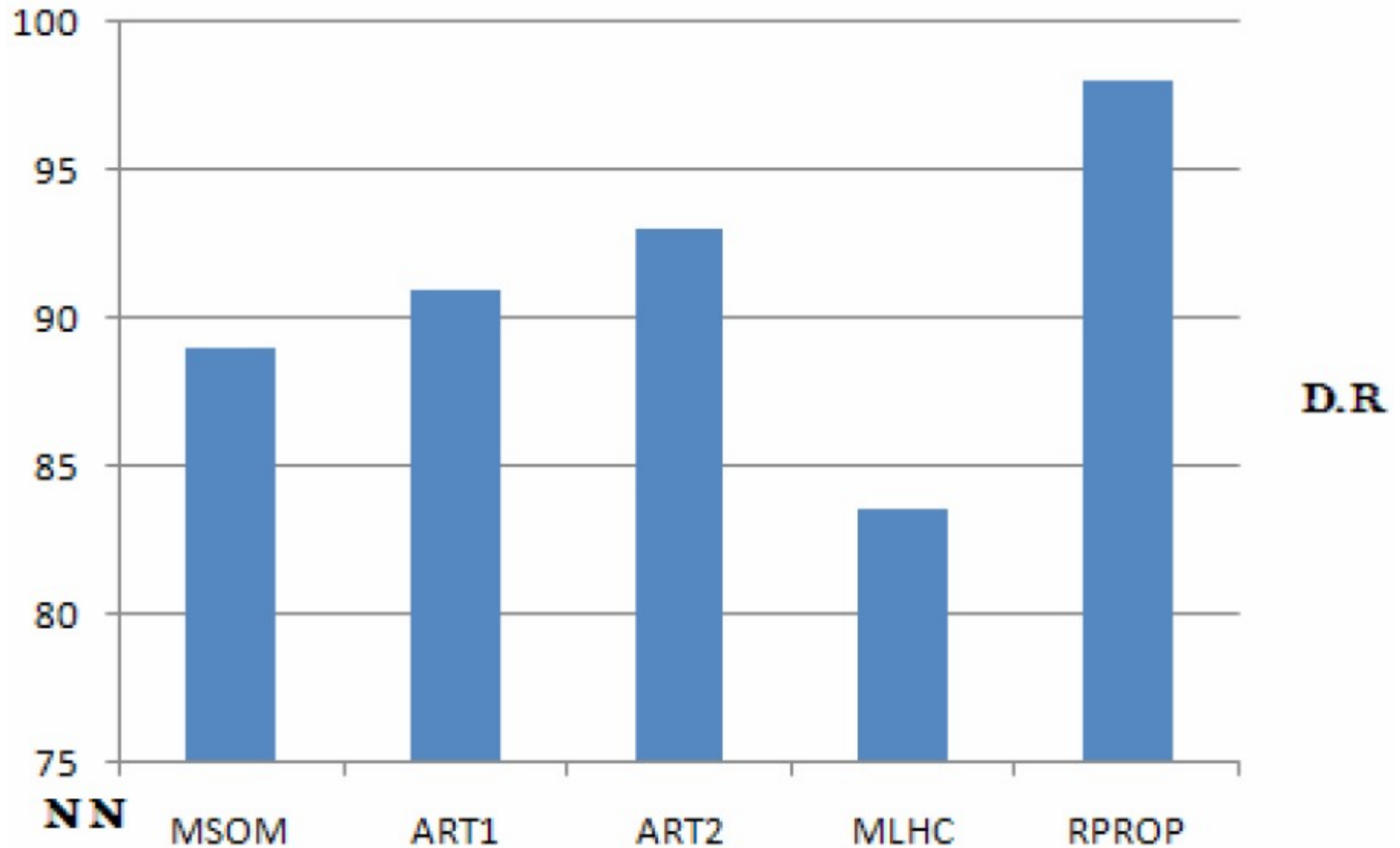
Training the NN

- Teacher layer used during training
 - Used to transmit the error difference backward through the network.
- 1000 epochs of a subset of the data set.
- Multiple NN architectures were trained.
 - Final arch chosen has smallest RMSE.
- Multiple activation functions were used
 - Final function had largest detection rate.

NN Arch Training Results

Sr.#	Hidden Layers	Neurons	RMSE
1	H1 → H2 → H3	14 → 9 → 3	0.1487
2	H1 → H2 → H3 → H4	14 → 9 → 6 → 3	0.1523
3	H1 → H2 → H3	14 → 9 → 4	0.01486
4	H1 → H2 → H3	20 → 10 → 5	0.1942
5	H1 → H2 → H3	30 → 25 → 15	0.5632
6	H1 → H2	14 → 9	0.00211
7	H1	30	0.1342

NN Arch Training Results



Testing

- Validation:
 - Training data sets run on final NN.
 - Ensure results match desired output.
- Recall / Generalization:
 - NN run with additional data
 - Used to determine effectiveness of NN on data it has not seen.

NN Recall Results

DOS Attack Type	Detection Rate	False Positives	False Negatives
Back	100 %	0 %	0 %
Land	100 %	0 %	0 %
Neptune	100 %	0 %	0 %
Pod	99 %	1 %	0 %
Smurf	99 %	1 %	0 %
Teardown	79 %	15 %	6 %