

Traffic Analyzer

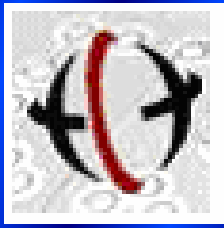
Prepared by: Devi Parikh

CMU Team:

Devi Parikh, Li-Hao Liu, Tsuhan Chen

Date: November 10, 2005

AMP
Advanced Multimedia Processing Lab



Overview

- Motivation
- Objective
- Algorithm
- System Layout
- Demonstration
- Conclusions
- Questions

Motivation

Objective

Algorithm

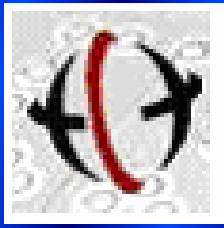
System -

Layout

Demo

Conclusion

Questions



Motivation



Motivation

Objective

- Intrusion detection in computer networks

Algorithm

System -

Layout

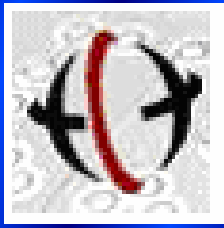
Demo

- Trade off between false alarm rates and ability to detect new attacks

Conclusion

- Pattern recognition can strike a balance

Questions



Objective

- Neural network based classification system
- Ensemble of classifiers approach
- Combine information from multiple sources (use most informative sources for different attack types)
- Adapt to changing traffic patterns

Motivation

Objective

Algorithm

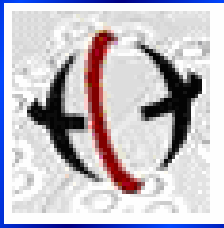
System -

Layout

Demo

Conclusion

Questions



Algorithm

Motivation

Objective

Algorithm

System -

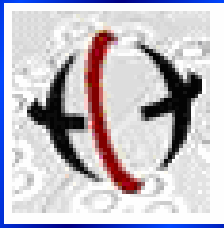
Layout

Demo

Conclusion

Questions

- Classification system
 - Subsections corresponding to each of the categories (normal, different attack types)
 - Subsections corresponding to each of the sources of information
 - Building blocks – Neural Networks



Algorithm

Input: Data split into **Training and Validation**

Output: Trained classification system

For each class

For each feature set (source of information)

Loop1: Train 1st NN on 2/3 of training data

Validation performance = $V1$

If $V1 < 0.5$ - Goto Loop1

Calculate weight

Loop2: Train 2nd NN on 2/3 of training data

Validation performance = $V2$

If $V2 < 0.5$ - Goto Loop2

Calculate weight

Validation of two networks combined = $V12$

If $V12 < V1$ - Goto Loop2

End

End

Motivation

Objective

Algorithm

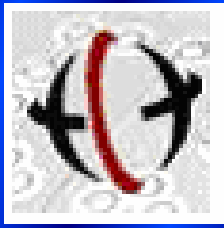
System -

Layout

Demo

Conclusion

Questions



Algorithm

Input: **Testing** dataset

Output: Classification decision

For each instance

Combine NN within sources – Weighted Sum Rule

Combine decisions within categories – Product Rule

If exactly one decision is positive

Pick corresponding class as decision

Elseif more than one are positive

Pick class with highest confidence

Elseif all decisions are negative

Raise an alert

Expert involvement to provide label

Update system by adding subsystem

End

End

Motivation

Objective

Algorithm

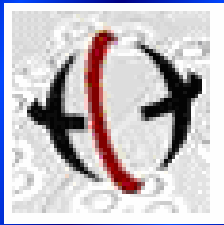
System -

Layout

Demo

Conclusion

Questions



System Layout

Motivation

Objective

Algorithm

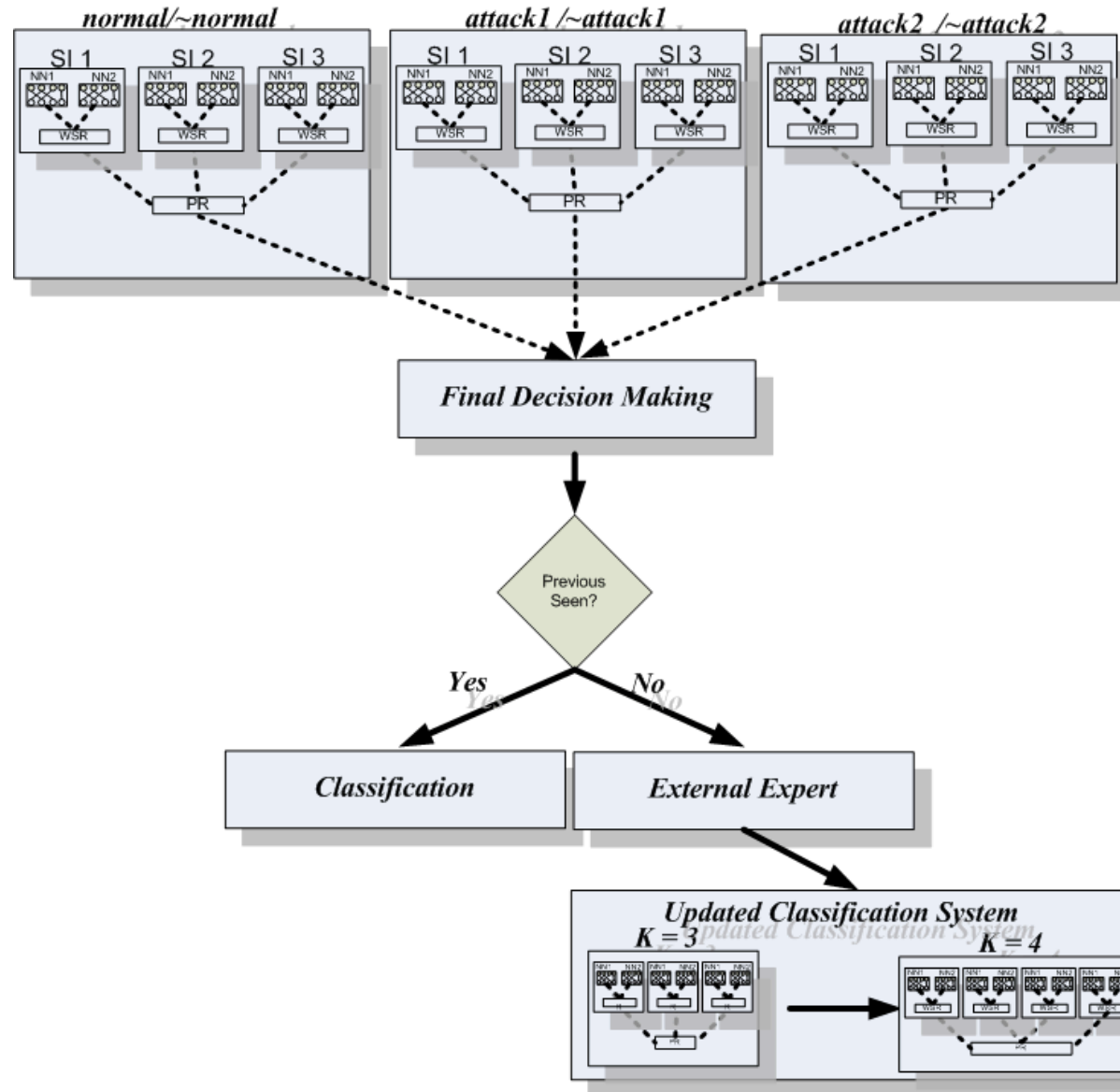
System -

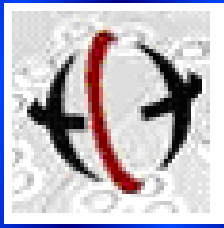
Layout

Demo

Conclusion

Questions





Demonstration

Demonstration (Testing) set up:

- KDD (MIT – DARPA, 1998) database
- 5 classes
 - Attack type 1: DOS
 - Attack type 2: PROBE
 - Attack type 3: U2R
 - Attack type 4: R2L
 - No attack: Normal
- Number of instances: 250 (50 per class)
- 3 sources of information
 - Source 1: Basic features
 - Source 2: Content features
 - Source 3: Traffic features
- Total of 30 neural networks in the classification system

Motivation

Objective

Algorithm

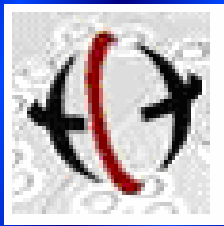
System -

Layout

Demo

Conclusion

Questions



Demonstration

Motivation

Objective

Algorithm

System -

Layout

Demo

Conclusion

Questions

```
MATLAB
File Edit Debug Desktop Window Help
C:\Documents and Settings\jparikh\My Documents\My Folder\Research\WorkInProgress\III Demo
Shortcuts How to Add What's New
Command Window
>> III_demo
Classification via fusion ...

Total of 250 instances classified into 5 categories: DOS, PROBE, U2R, R2L and NORMAL
Original distribution - 50 instances from each class

Would you like to view individual classification results (C) or aggregate statistics (A)? |
Start Waiting for input OVR
```



Demonstration

Motivation

Objective

Algorithm

System -

Layout

Demo

Conclusion

Questions

```
MATLAB
File Edit Debug Desktop Window Help
C:\Documents and Settings\dparikh\My Documents\My Folder\Research\WorkInprogress\III Demo
Shortcuts How to Add What's New
Command Window
>> III_demo
Classification via fusion ...

Total of 250 instances classified into 5 categories: DOS, PROBE, U2R, R2L and NORMAL
Original distribution - 50 instances from each class

Would you like to view individual classification results (C) or aggregate statistics (A)? C

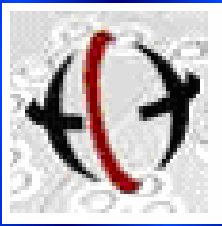
Enter number of instances to be viewed simultaneously: 1

----- INSTANCE NUMBER: 1 -----
Basic   features: 0 2 12 10 105 146 0 0 0
Content features: 0 0 0 0 0 0 0 0 0 0 0 0
Traffic features: 1 1 0 0 0 0 1 0 0 255 252 0.99 0.01 0 0 0 0 0 0
Assigned to R2L      Correct label: R2L      Cost: 0

-----

Would you like to continue?
Enter (Y) to view more individual classification results or (N) to skip to aggregate statistics ...

Start Waiting for input
```



Demonstration

Motivation

Objective

Algorithm

System -

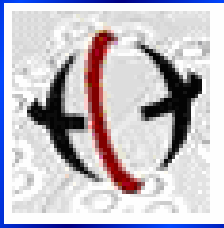
Layout

Demo

Conclusion

Questions

```
Enter (Y) to view more individual classification results or (N) to skip to aggregate statistics ... N
***** AGGREGATE STATISTICS *****
Number of instances classified as DOS: 54
Number of instances classified as PROBE: 47
Number of instances classified as U2R: 50
Number of instances classified as R2L: 49
Number of instances classified as NORMAL: 50
Percentage correct classification 93.2%
False alarms rate 1.5%
Missed attacks rate 6%
Aggregate Cost per instance is 0.144
*****
>>
```



Current Status

- Database analyzed and set up
- Identified most informative sources of information for each attack type
- Working prototype
- Data fusion incorporated
- Comparable classification performance

Motivation

Objective

Algorithm

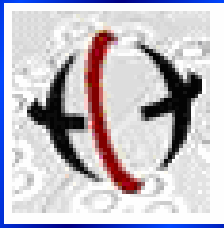
System -

Layout

Demo

Conclusion

Questions



Motivation

Objective

Algorithm

System -

Layout

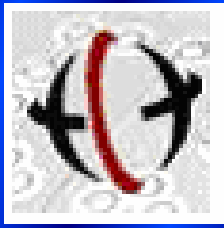
Demo

Conclusion

Questions

Future work

- Incorporate adaptability
- Incorporate fine tuning towards minimizing the cost function
- Computationally efficient



Summary

Motivation

Objective

Algorithm

System -

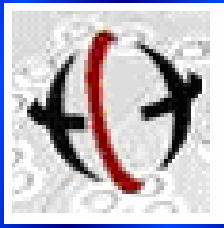
Layout

Demo

Conclusion

Questions

- Pattern recognition techniques for intrusion detection
- Neural networks
- Data fusion
- Adaptability



Motivation

Objective

Algorithm

System -

Layout

Demo

Conclusion

Questions

Questions?