

Intrusion Detection with Genetic Algorithms and Fuzzy Logic

Emma Ireland

Division of Science and Mathematics
University of Minnesota, Morris
Morris, Minnesota, USA

December 2013
UMM CSci Senior Seminar Conference

The big picture



Outline

- 1 Background
- 2 Genetic Algorithm Implementation
- 3 Fuzzy Genetic Algorithm Implementation
- 4 Conclusions

Outline

- 1 Background
 - Types of Networking Attacks
 - Detection Methodologies
 - Data Sets
 - Rules
 - Fuzzy Logic
 - Genetic Algorithm
 - Determining the accuracy of an algorithm

2 Genetic Algorithm Implementation

3 Fuzzy Genetic Algorithm Implementation

4 Conclusions

title here

title

title

title

title

title

title

Outline

- 1 Background
- 2 Genetic Algorithm Implementation
 - Algorithm Overview
 - Experimental Design and Results
- 3 Fuzzy Genetic Algorithm Implementation
- 4 Conclusions

title here

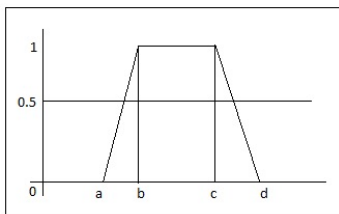
title

Outline

- 1 Background
- 2 Genetic Algorithm Implementation
- 3 Fuzzy Genetic Algorithm Implementation
 - Fuzzy Algorithm
 - Algorithm Overview
 - Experimental Design and Results
- 4 Conclusions

Measuring the probability of a record being an attack

- Trapezoidal shape



- The parameters are the values of a feature.

- Fuzzy algorithm

if data value is between b and c **then**
 $\text{prob} = 1.0$

else if data value is between a and b
then

$$\text{prob} = (\text{data} - a) / (b - a)$$

else if data value is between c and d
then

$$\text{prob} = (d - \text{data}) / (d - c)$$

else

$$\text{prob} = 0.0$$

end if

Encoding of features and rules

- The four parameters are encoded into blocks.
- Each block is a feature with values between 0.0 and 7.0.

010	011	100	101
a=2	b=3	c=4	d=5

- A rule has 12 blocks of features, at the end is the type of attack.

010	011	100	101	010	011	101	111	DoS
a=2	b=3	c=4	d=5	a=2	b=3	c=5	d=7	
Block 1					Block 12				Type

title

title

Outline

- 1 Background
- 2 Genetic Algorithm Implementation
- 3 Fuzzy Genetic Algorithm Implementation
- 4 Conclusions**

Conclusions



Thanks!

Thank you for your time and attention!

Questions?

References