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

Outline

title here

title

KDD99

- Generated by simulating a military network environment in 1999.
- Has long been a standard data set for intrusion detection.
- Data in the set is classified as normal or attack activity.

- KDD99 uses 41 features.
  - *Features* are properties of a *record*, (either an attack or normal activity), that are used to describe the activity.

Some features of KDD99

1. duration: length of the normal or attack activity in seconds.
2. src_bytes: number of bytes sent from source to destination.
3. num_failed_logins: number of failed login attempts.
4. root_shell: returns 1 if root shell is obtained, else returns 0.
5. num_access_files: number of operations on access control files.
6. srv_count: number of connections to the same service as the current connection in the past two seconds.
7. serror_rate: percentage of connections that have “SYN" errors.
8. same_srv_rate: percentage of connections to the same service.

RLD09

title

title

title

title

Outline

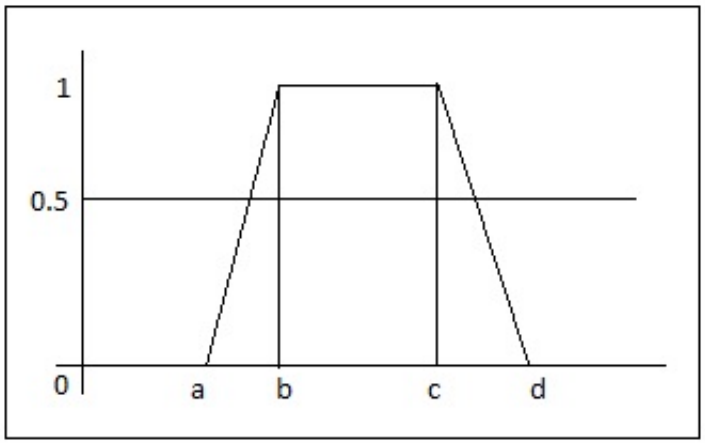
title here

title

Outline

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**
  prob = 1.0
else if data value is between *a* and *b* **then**
  prob = $(\text{data} - a)/(b - a)$
else if data value is between *c* and *d* **then**
  prob = $(d - \text{data})/(d - c)$
else
  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

Conclusions

-
-
-

Thanks!

Thank you for your time and attention!

Questions?

References