

# **Decision Trees vs. Neural Networks for Intrusion Detection**

Yacine Bouzida  
Bouzida@tcl.ite.mee.com

**IEEE/IST Workshop on  
"Monitoring, Attack Detection and Mitigation"**

Thursday 28 / Friday 29 September, 2006  
Tuebingen, Germany

## 1. Problems

- ◆ 3-6 new vulnerabilities per day (1000-2000 per year)
- ◆ New attack forms
- ◆ Existing methods cannot detect these new attacks

## 2. Objectives

- ◆ Detection of new attacks
- ◆ New methods to detect these new attacks



## 1. Intrusion Detection

1.1 Introduction

1.2 Detection techniques

## 2. Motivations and New Attacks Detection

## 3. Experimentation

## 4. Conclusion and Perspectives

# 1. Intrusion Detection

---

## ■ Intrusion

- *A finite and not empty set of actions that attempt to violate the security policy of an information system (system or network resource)*
- Intrusion detection
  - A process which permits to identify and respond to intrusions
- ⇒ Monitor the information system to detect
  - ▶ External attacks
  - ▶ Internal Intrusions
  - ▶ Anomalies
- Prevention techniques
  - ◆ Access control
  - ◆ Cryptography, ...

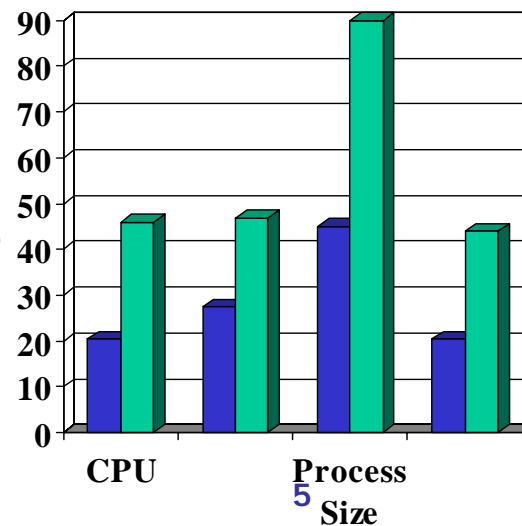
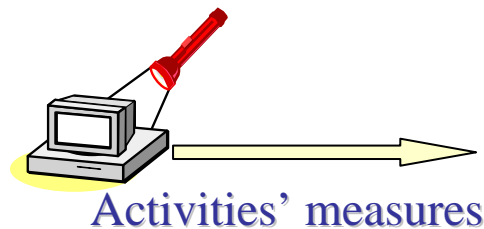
# 1. Intrusion Detection

## ■ Two different techniques

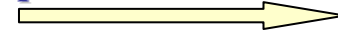
- ▶ Anomaly based
- ▶ Misuse based

## ■ Anomaly based

- ▶ Two steps (Learning, detection) in general
- ▶ Detection of a behavior deviation (user, application, network traffic, ...) from its reference profile



probable intrusion



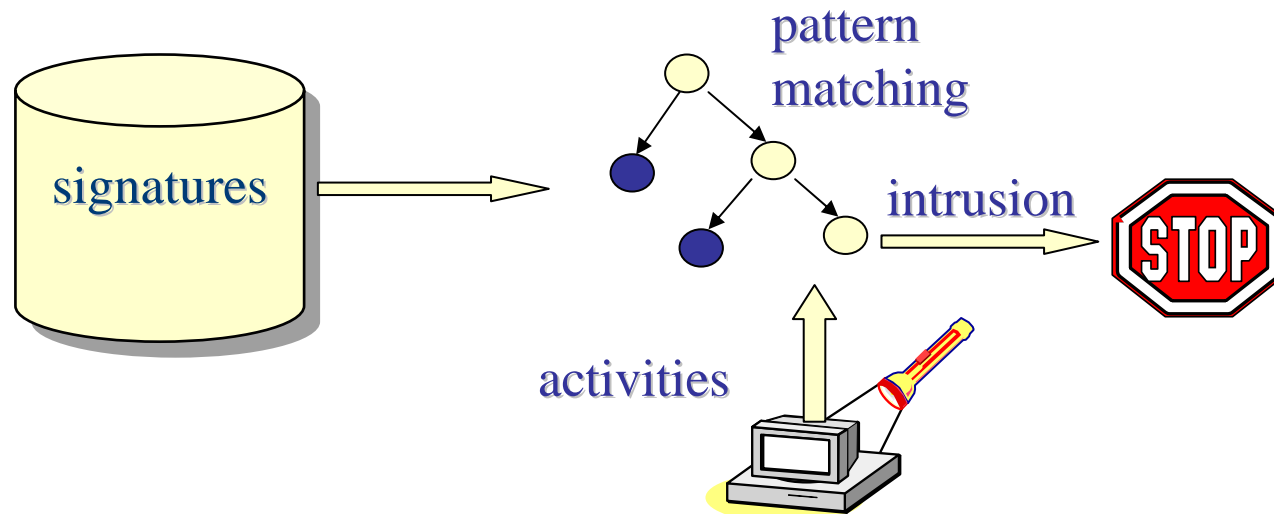
- normal profile
- abnormal



# 1. Intrusion Detection

- Misuse detection

- ▶ A set of attacks or at least litigious actions described in the signature database



## 1. Intrusion Detection

## 2. Motivations and New Attacks Detection

### 2.1 Motivations

### 2.2 Neural Networks

- Improvement for new attacks' detection

### 2.3 Decision trees

- Improvement for new attacks' detection

## 4. Experimentation

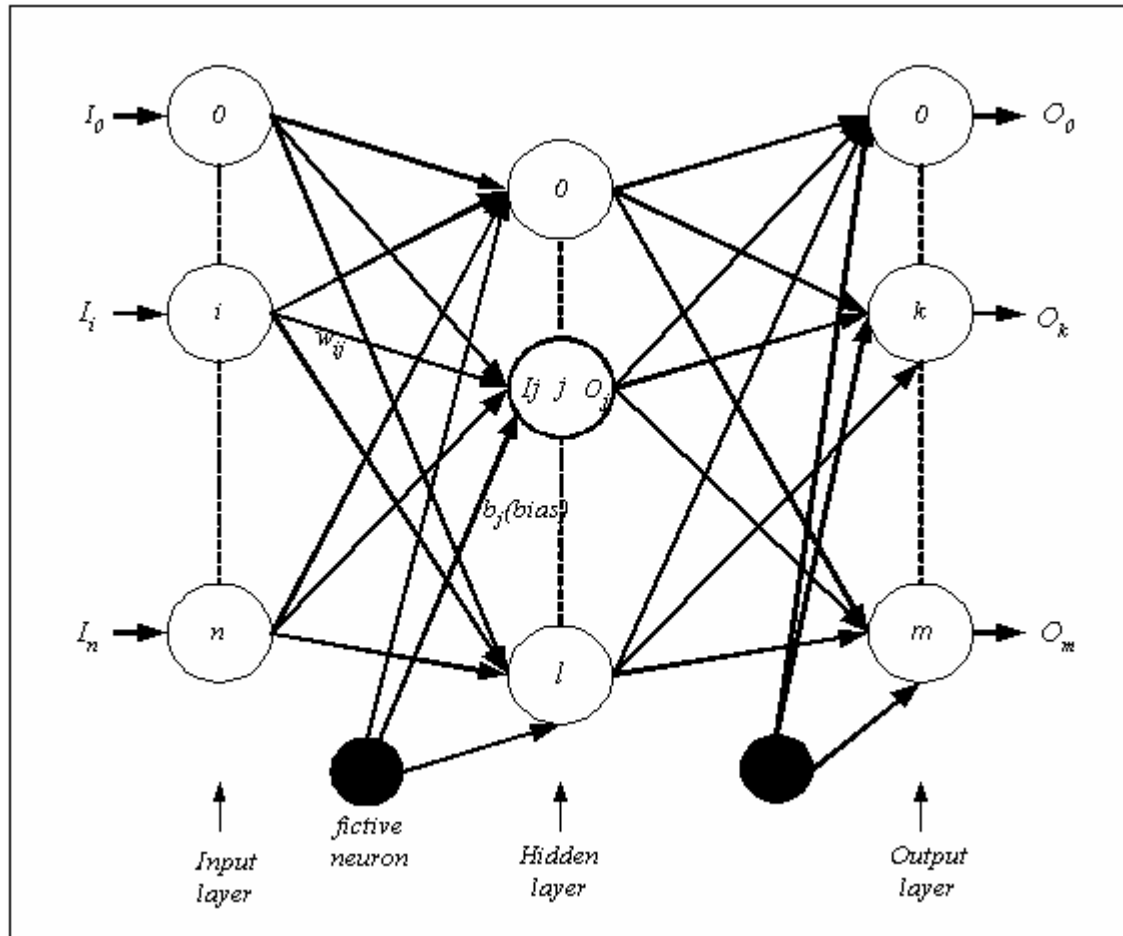
## 5. Conclusion and perspectives

#### ■ Limits of current IDSs

- ▶ Anomaly detection
  - ◆ An anomaly may be just a new normal activity
  - ◆ High false positive rates
  - ◆ Not well specified for network traffic
  
- ▶ Misuse detection
  - ◆ High false negative rates
    - Polymorphic attacks
    - New attacks
  - ◆ High false positive rates
    - Attacks not well specified

- Limits of the supervised techniques
  - ▶ Only known instances may be predicted
- Known attacks are not considered by anomaly detection techniques
  
- Improving the anomaly detection approach
  - ▶ Learn
    - ◆ the normal profile (reference)
    - ◆ a priori known attacks
  - ▶ A new audited profile is classified as
    - ◆ normal,
    - ◆ abnormal and the corresponding anomaly is known, or
    - ◆ new,
      - considered momentarily as a new attack
      - a diagnosis is necessary

- Multilayer Neural Networks
  - Principle



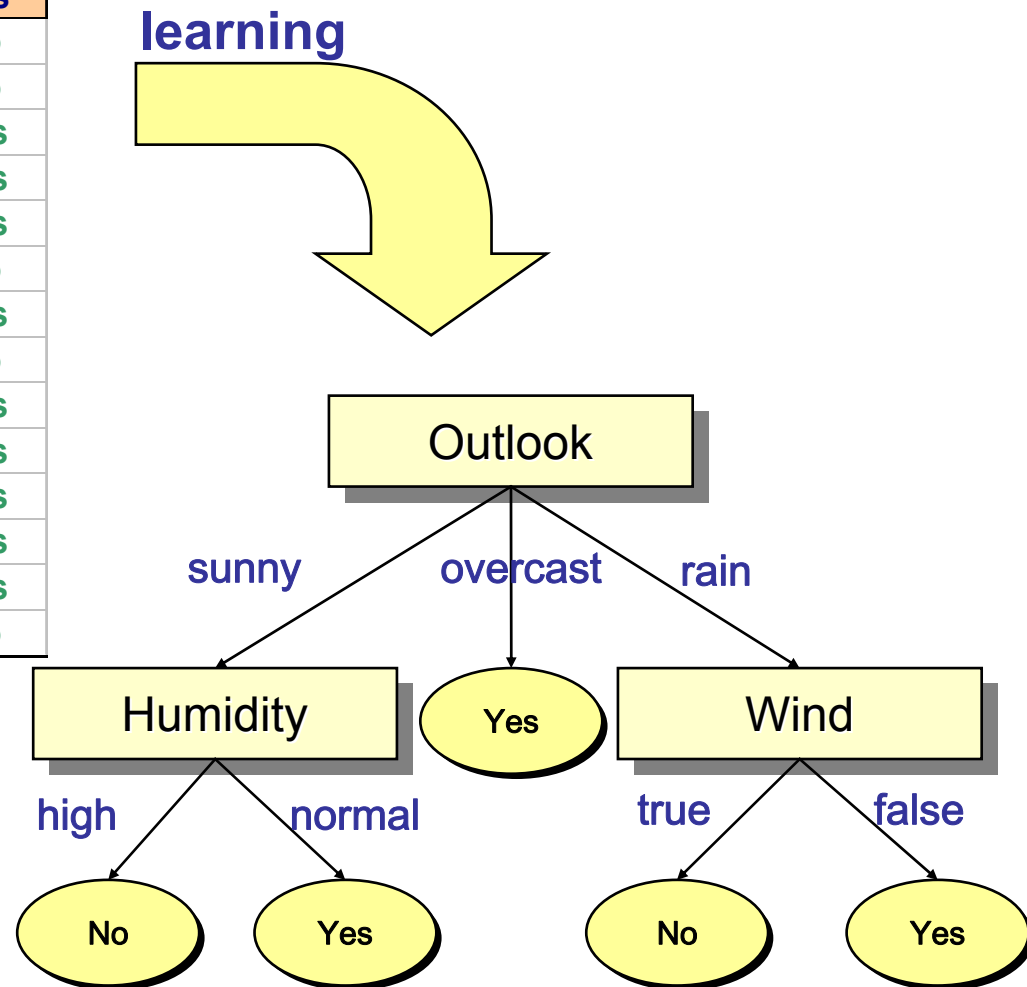
### ■ Neural Networks

- ◆ Classification
  - The class corresponding to the highest activated neuron in the output layer
  
- ◆ Improvement
  - IF (all the values of the output layer  $\leq \theta$ )
    - ◆ New connection
    - ◆ Considered momentarily new attack
    - ◆ Diagnostic
  - ELSE
    - ◆ Let the  $k^{th}$  neuron be the most activated
    - ◆ This connection corresponds to the  $k^{th}$  class
  - Fi

- Mechanism
  - ▶ Top Down Strategy based on the "divide and conquer" approach where the major aim is to partition the tree into many subsets mutually exclusive
  - ▶ Each sub partition corresponds to a sub-problem classification
  
- Decision tree components
  - ▶ Node: specifying the test attribute
  - ▶ Edge (branch): a possible attribute value
  - ▶ Leaf (answer node): designed classification class
  
- Learning step (building the tree)
- Classification step

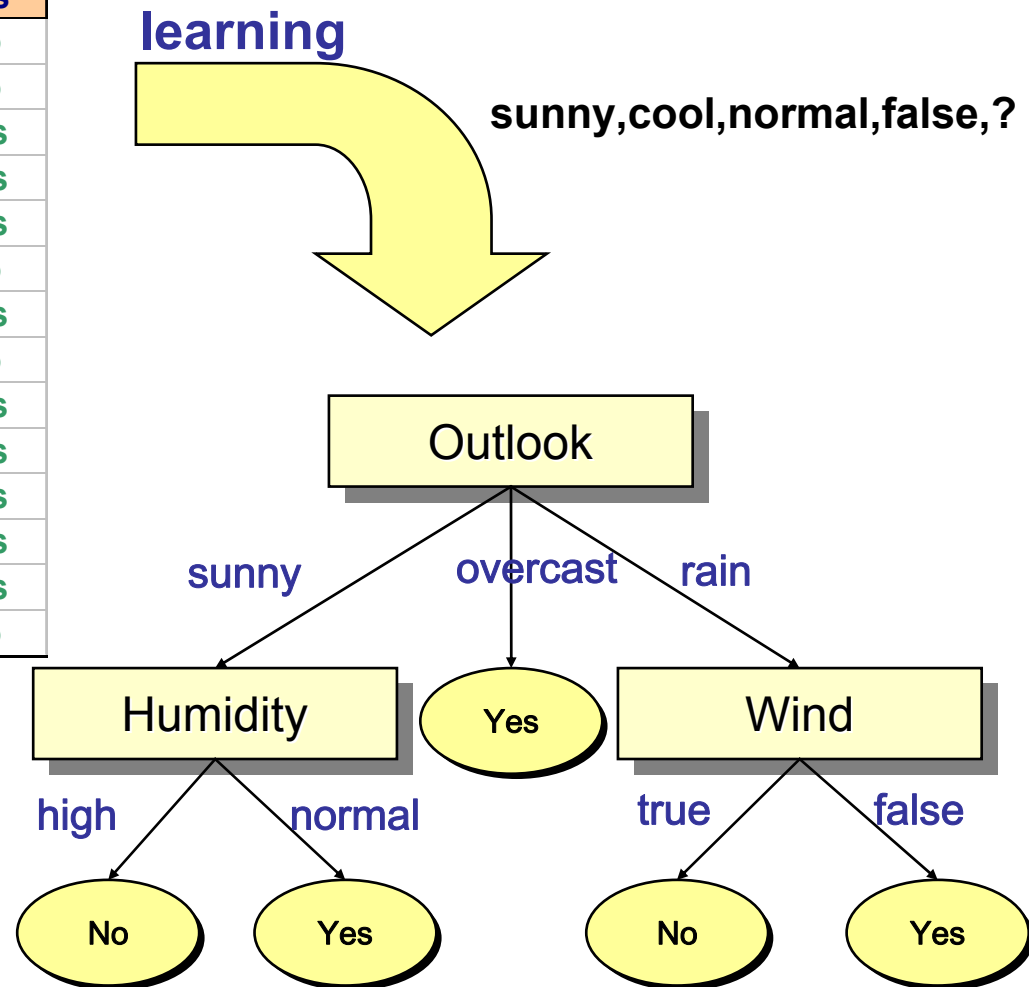
#### Learning step

N°	Outlook	Temperature	Humidity	wind	Class
1.	sunny	hot	high	false	No
2.	sunny	hot	high	true	No
3.	overcast	hot	high	false	Yes
4.	rain	mild	high	false	Yes
5.	rain	cool	normal	false	Yes
6.	rain	cool	normal	true	No
7.	overcast	cool	normal	true	Yes
8.	sunny	mild	high	false	No
9.	sunny	cool	normal	false	Yes
10.	rain	mild	normal	false	Yes
11.	sunny	mild	normal	true	Yes
12.	overcast	mild	high	true	Yes
13.	overcast	hot	normal	false	Yes
14.	rain	mild	high	true	No



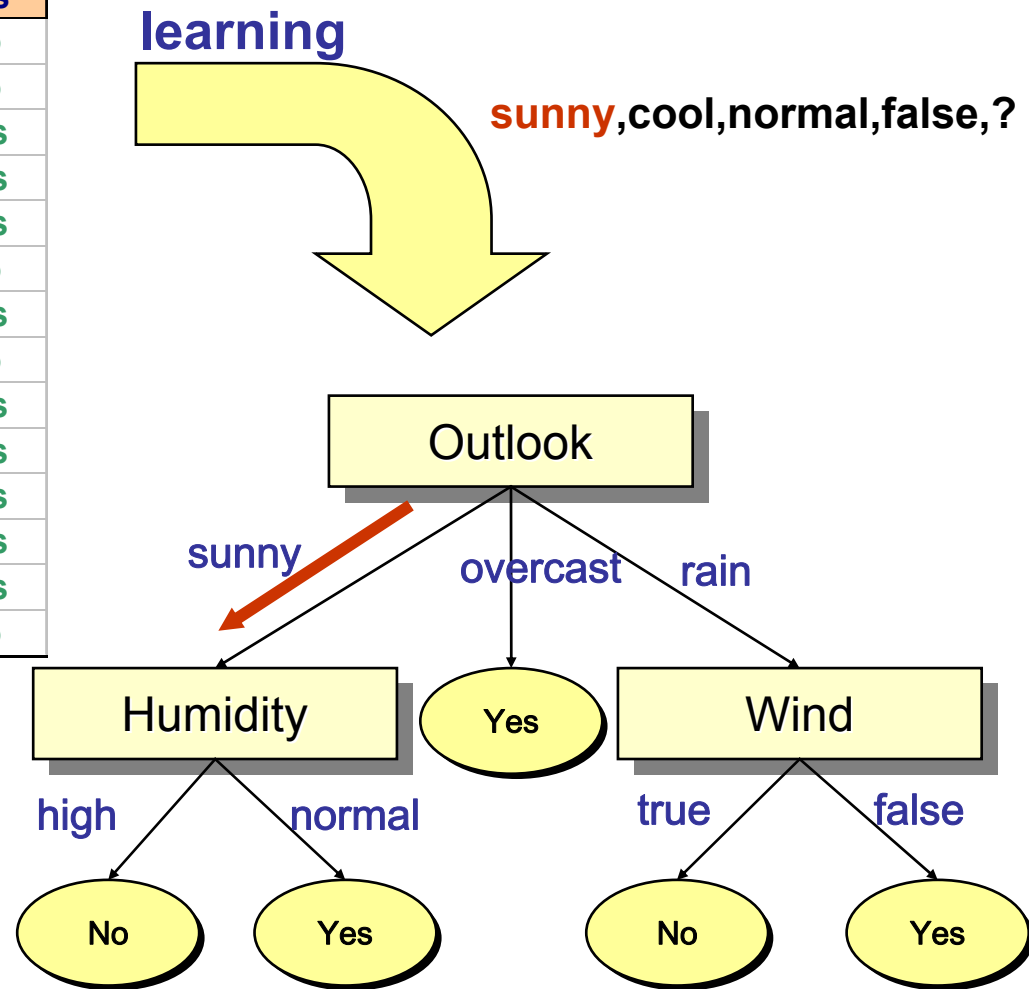
#### Learning step

N°	Outlook	Temperature	Humidity	wind	Class
1.	sunny	hot	high	false	No
2.	sunny	hot	high	true	No
3.	overcast	hot	high	false	Yes
4.	rain	mild	high	false	Yes
5.	rain	cool	normal	false	Yes
6.	rain	cool	normal	true	No
7.	overcast	cool	normal	true	Yes
8.	sunny	mild	high	false	No
9.	sunny	cool	normal	false	Yes
10.	rain	mild	normal	false	Yes
11.	sunny	mild	normal	true	Yes
12.	overcast	mild	high	true	Yes
13.	overcast	hot	normal	false	Yes
14.	rain	mild	high	true	No



### Learning step

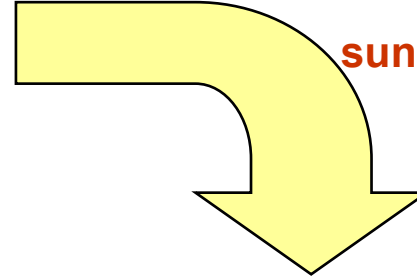
N°	Outlook	Temperature	Humidity	wind	Class
1.	sunny	hot	high	false	No
2.	sunny	hot	high	true	No
3.	overcast	hot	high	false	Yes
4.	rain	mild	high	false	Yes
5.	rain	cool	normal	false	Yes
6.	rain	cool	normal	true	No
7.	overcast	cool	normal	true	Yes
8.	sunny	mild	high	false	No
9.	sunny	cool	normal	false	Yes
10.	rain	mild	normal	false	Yes
11.	sunny	mild	normal	true	Yes
12.	overcast	mild	high	true	Yes
13.	overcast	hot	normal	false	Yes
14.	rain	mild	high	true	No



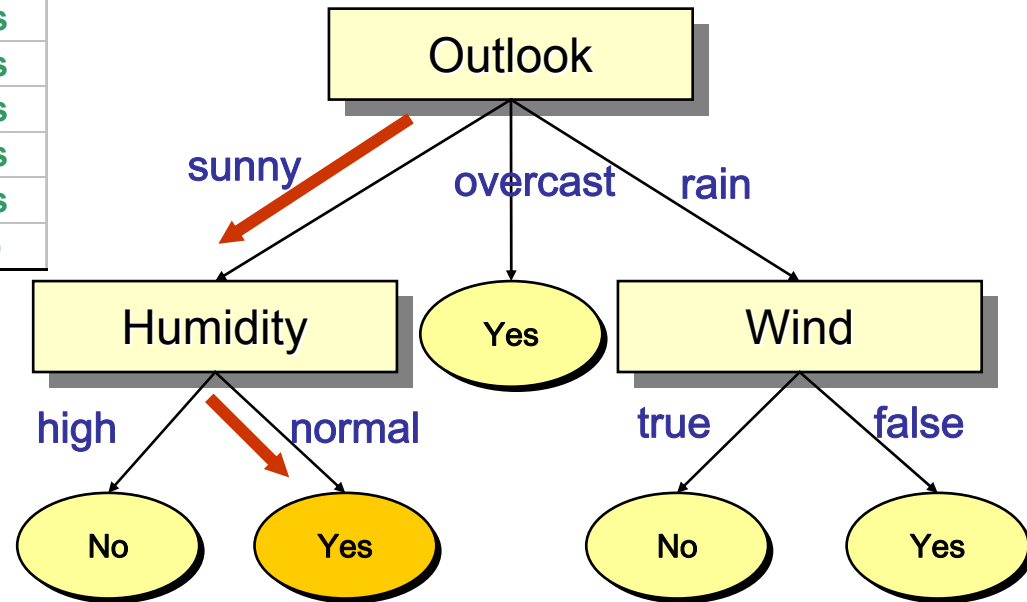
### Learning step

N°	Outlook	Temperature	Humidity	wind	Class
1.	sunny	hot	high	false	No
2.	sunny	hot	high	true	No
3.	overcast	hot	high	false	Yes
4.	rain	mild	high	false	Yes
5.	rain	cool	normal	false	Yes
6.	rain	cool	normal	true	No
7.	overcast	cool	normal	true	Yes
8.	sunny	mild	high	false	No
9.	sunny	cool	normal	false	Yes
10.	rain	mild	normal	false	Yes
11.	sunny	mild	normal	true	Yes
12.	overcast	mild	high	true	Yes
13.	overcast	hot	normal	false	Yes
14.	rain	mild	high	true	No

learning



sunny, cool, normal, false, Yes



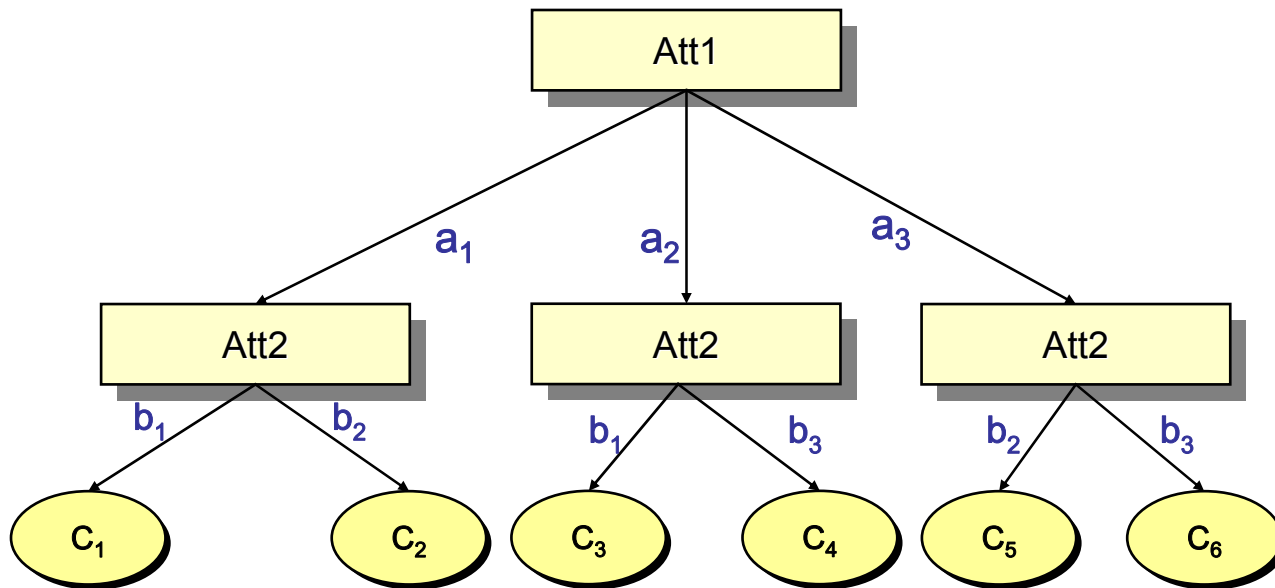
## Decision Trees

### ▶ C4.5rules

- ◆ Generating the rules from the decision trees
- ◆ Pruning

### ▶ Problem

- ◆ What happens if there is not a path from the root to the leaves
- ◆ New instances case



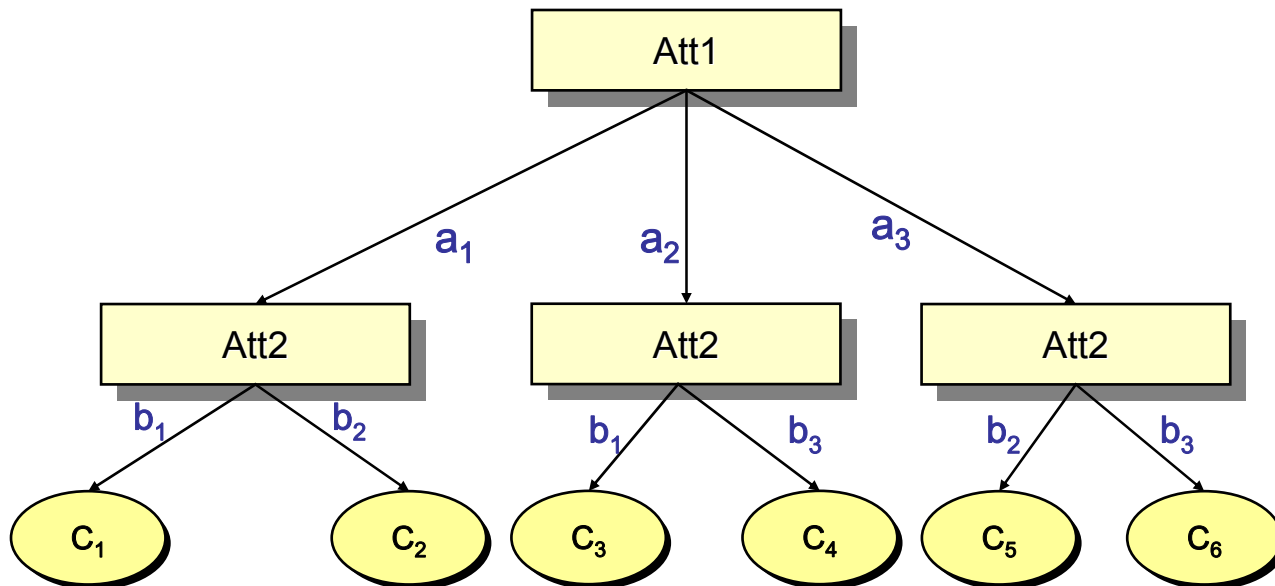
## Decision Trees

### ▶ C4.5rules

- ◆ Generating the rules from the decision trees
- ◆ Pruning

### ▶ Problem

- ◆ What happens if there is not a path from the root to the leaves
- ◆ New instances case



a1,b3, ?

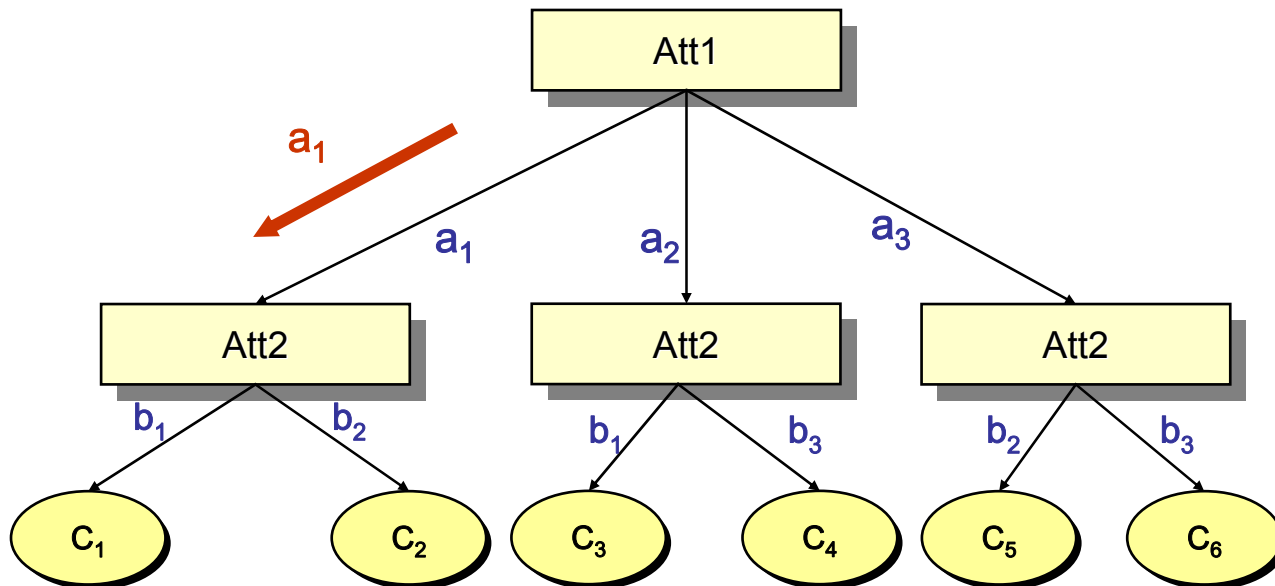
## Decision Trees

### ▶ C4.5rules

- ◆ Generating the rules from the decision trees
- ◆ Pruning

### ▶ Problem

- ◆ What happens if there is not a path from the root to the leaves
- ◆ New instances case



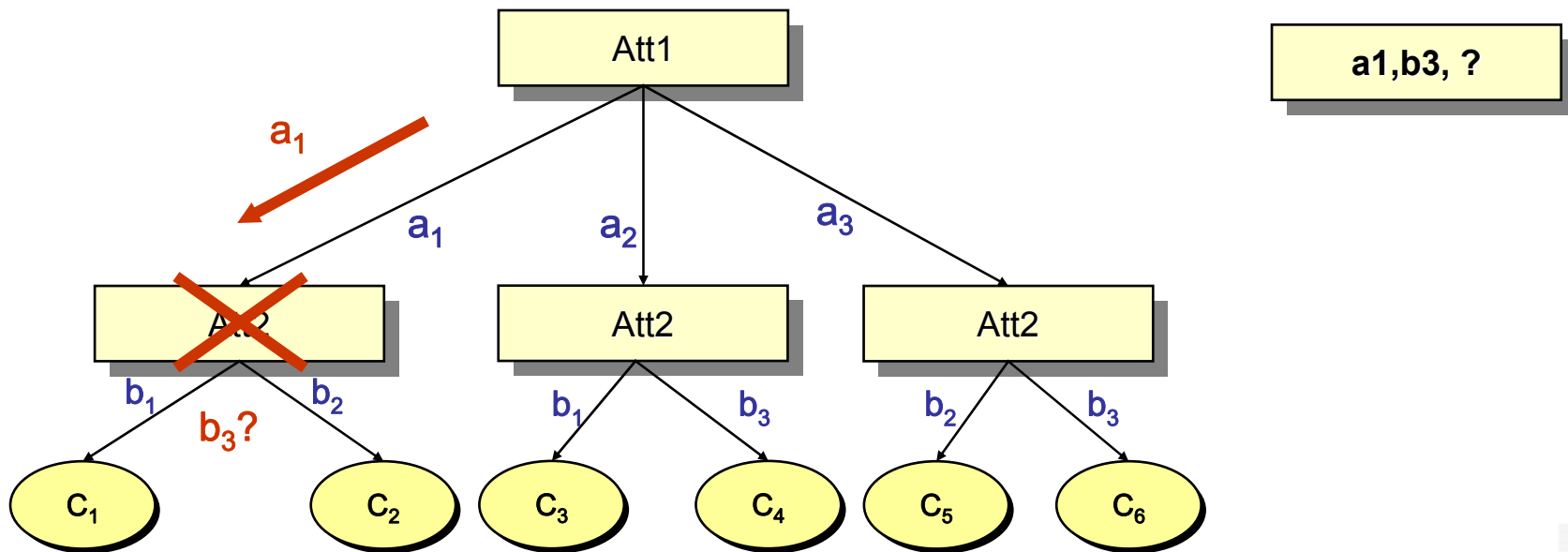
#### ■ Decision Trees

##### ▶ C4.5rules

- ◆ Generating the rules from the decision trees
- ◆ Pruning

##### ▶ Problem

- ◆ What happens if there is not a path from the root to the leaves
- ◆ New instances case



#### ■ Solution (Quinlan93)

- ◆ Default class
  - ◆ Corresponds to that containing the most items not covered by any rule
  - ◆ In case of conflict, ties are resolved in favor of the most frequent class
- 
- Example
    - ◆ IF (**duration  $\leq 2$  & num\_failed\_login  $> 5$** )  
THEN **guess\_passwd**
    - ◆ IF (**protocol\_type = icmp & src\_bytes  $> 300$**  )  
THEN **smurf**
    - ◆ Default : **normal**



- Enhancing the classification process
  - ◆ Classify new instances in class «New»
  
- Improving the anomaly approach is satisfied
  - ◆ The new class corresponds to the new behaviors class



## 1. Intrusion Detection

## 2. Motivations and New Attacks' Detection

## 3. Experimentation

3.1 KDD99 (DARPA98)

3.2 Neural Networks

3.3 Decision Trees

3.4 Critics over KDD99

3.5 Real network traffic

## 4. Conclusion and Perspectives

- Task :
  - ▶ Build a predictive model (i.e. a classifier) capable of distinguishing between «bad» connections, called intrusions or attacks, and «good» normal connections
  
- Data (connections)
  - ▶ Four gigabytes of compressed binary TCPdump data of network traffic (Lincoln Labs) processed into 5 million connection records of 41 attributes (discrete and continuous)

- Each connection is labeled either as normal or as an attack with exactly one attack type among 39 attacks gathered into 4 categories
  - ◆ **Probing (6)**: surveillance and other probing, port scanning (nmap, satan ...)
  - ◆ **DoS (10)**: Denial of Service (syn flooding, smurfing ...)
  - ◆ **U2R (8)**: unauthorized access to local superuser (root) privileges (buffer overflow attacks).
  - ◆ **R2L (15)**: unauthorized access from a remote machine (password guessing)
  
- Learning Dataset
  - ◆ ~5 million connections (only 10% (494,021) are used)
  
- Test Dataset
  - ◆ 311,029 connections

- Attacks percentages of each category in each dataset

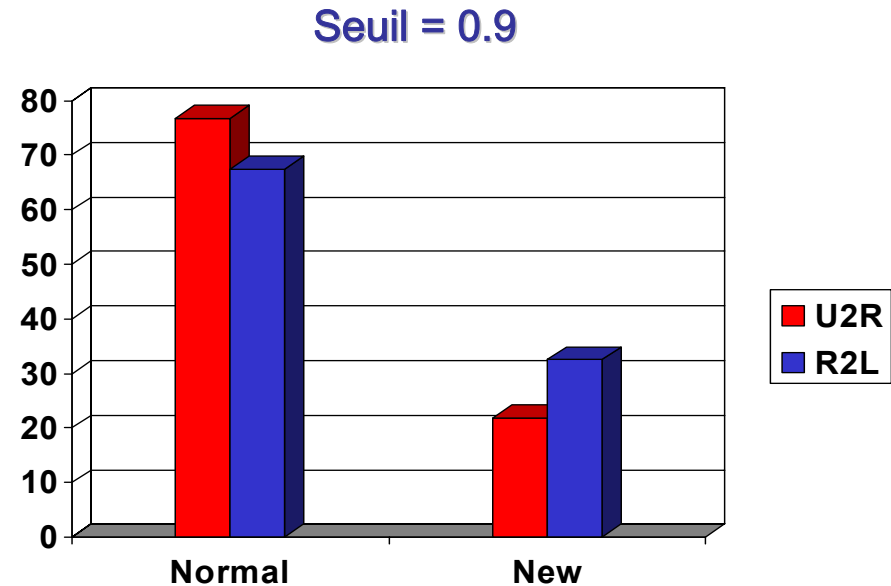
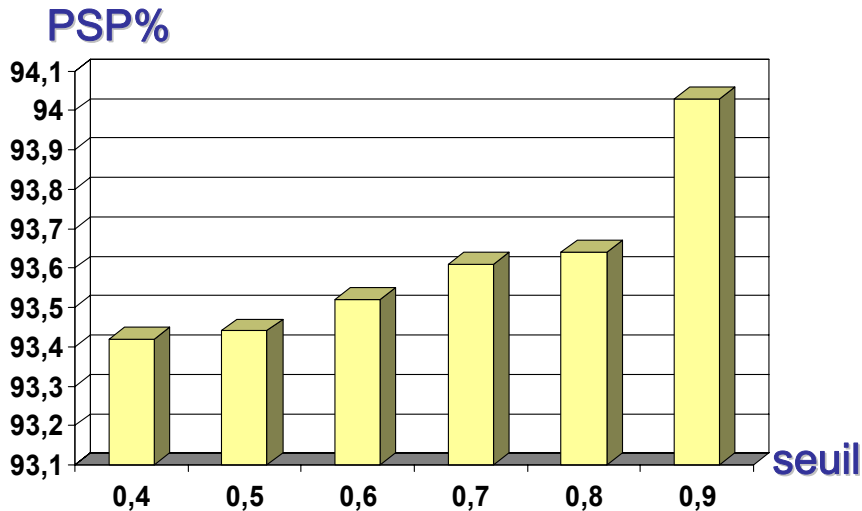
	Learning Dataset Connections		Test Dataset Connections	
	%	# Attacks	%	# New Attacks
Normal	19.69%	-	19.48%	-
Probing	0.83%	4	1.34%	2 (42.94%)
DoS	79.24%	6	73.90%	4 (2.85%)
U2R	0.01%	4	0.07%	4 (92.90%)
R2L	0.23%	8	5.20%	7 (63%)

- DARPA 98/99 datasets are criticized but are always highly used to evaluate current research in intrusion detection

### Results (without threshold)

Predicted Effective	Normal	Probing	DoS	U2R	R2L
Normal(60.593)	<b>97.87%</b>	0,75%	1,20%	0,00%	0,18
Probing(4.166)	10,68%	<b>71,63%</b>	15,34%	0,00%	2,35
DoS(229.853)	2,62%	0,36%	<b>97,00%</b>	0,00%	0,02
U2R(228)	86,84%	7,02%	3,95%	<b>0,00%</b>	2,19%
R2L(16.189)	93,20%	0,06%	0,06	0,00%	<b>26,68%</b>
<b>PSP=93,10</b>					

### Results (with threshold)



- Best results over KDD 99
- Most of U2R et R2L connections
  - ◆ Classified as normal

### Standard C4.5rules

Predicted	Normal	Probing	DoS	U2R	R2L
<b>Effective</b>					
Normal (60.593)	<b>99,47%</b>	0,40%	0,12%	0,01%	0,00%
Probing (4.166)	18,24%	<b>72,73%</b>	2,45%	0,00%	6,58%
DoS (229.853)	2,62%	0,06%	<b>97,14%</b>	0,00%	0,18%
U2R (228)	82,89%	4,39%	0,44%	<b>7,02%</b>	5,26%
R2L (16.189)	81,60%	14,85%	0,00%	0,70%	<b>2,85%</b>
<b>PSP=92,30%</b>					

### Enhanced C4.5rules

Predicted	Normal	Probing	DoS	U2R	R2L	New
<b>Effective</b>						
Normal (60.593)	<b>99,43%</b>	0,40%	0,12%	0,01%	0,00%	<b>0,04%</b>
Probing (4.166)	8,19%	<b>72,73%</b>	2,45%	0,00%	6,58%	10,05%
DoS (229.853)	2,26%	0,06%	<b>97,14%</b>	0,00%	0,18%	0,36%
U2R (228)	21,93%	4,39%	0,44%	<b>7,02%</b>	5,26%	<b>60,96%</b>
R2L (16.189)	<b>79,41%</b>	14,85%	0,00%	0,70%	<b>2,85%</b>	<b>2,20%</b>
<b>PSP=(92,30+0,57)%</b>						

### ■ Problem

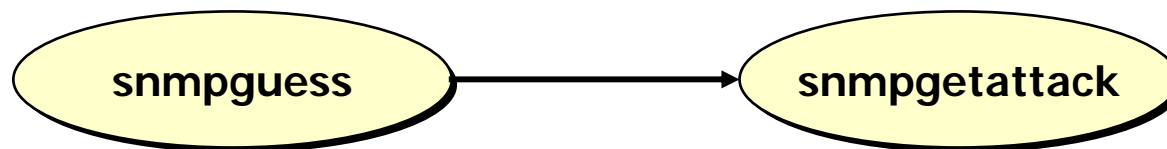
- ▶ PSP initial (before improving the classification process)
  - ◆ 92,30%
- ▶ PSP when using the *new* class
  - ◆ 92,87%
  - ◆ less high as expected
- ▶ R2L
  - ◆ 79,41% connections are predicted as a normal traffic
  - ◆ A possible Explanation
    - snmpguess (26,75% : 4.367/16.189)
    - snmpgetattack (47,82% : 7.741/16.189)

### ■ SNMPGUESS

- ▶ Guesses the password of the SNMP community using the dictionary attack

### ■ SNMPGETATTACK

- ▶ Monitors the SNMP community using the password guessed by *snmpguess*
  - ▶ Difficult to detect (password usurped)
- ### ■ Alert correlation may be used



- *snmpguess* attack remains undetectable using misuse based techniques

- R2L Problem

- ▶ Test 2

- ◆ The KDD99 test database is used as a learning test data base

- ▶ Result

Predicted Effective	Normal	Probing	DoS	U2R	R2L	New
Normal (60.593)	<b>98,34%</b>	0,02%	0,03%	0,01%	1,50%	0,11%
Probing (4.166)	0,19%	<b>99,35%</b>	0,07%	0,00%	0,00%	0,38%
DoS (229.853)	0,01%	0,00%	<b>99,99%</b>	0,00%	0,00%	0,00%
U2R (228)	2,19%	0,00%	0,00%	<b>96,93%</b>	0,00%	0,88%
R2L (16.189)	36,40%	0,02%	0,01%	0,05%	<b>63,33%</b>	0,19%
<b>PSP=97,70%</b>						

- Learned instances are not correctly classified for the R2L class

- ◆ Ratio of classification with success : 63,33%

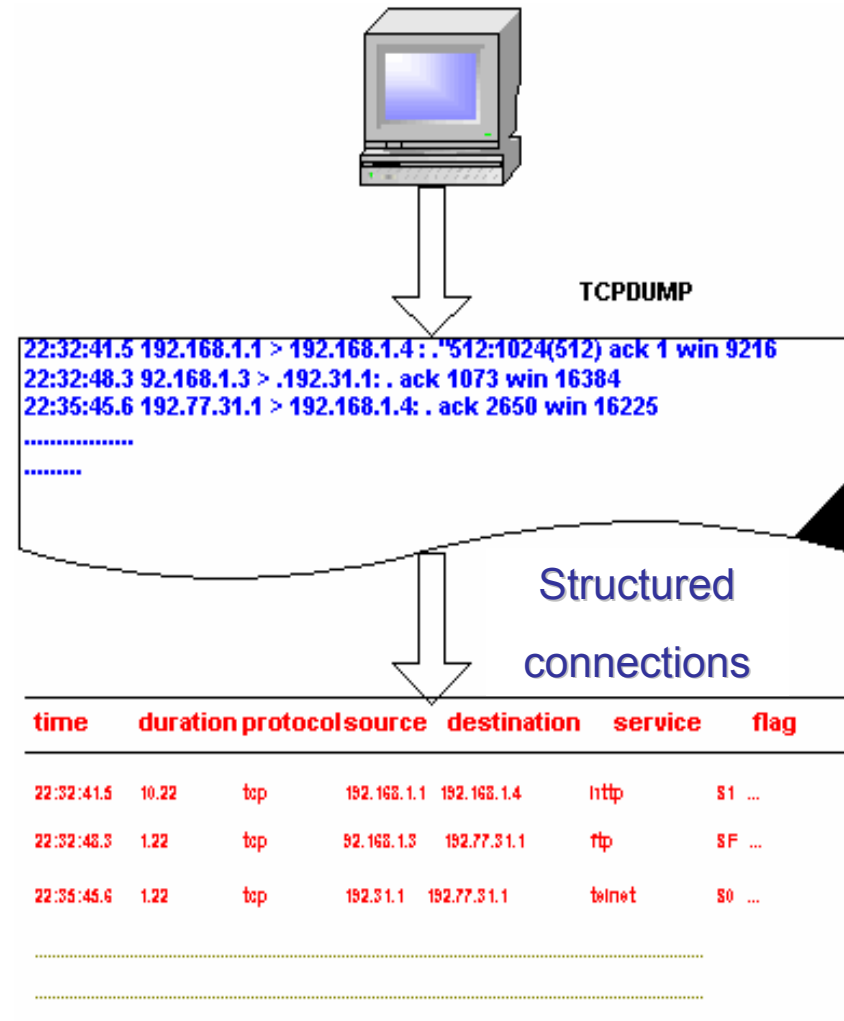
- ◆ SNMPGETATTACK (7741)

- 71,85% : Normal , 27,96% : R2L et 0,19% : new

- The transformation function used in KDD99
  - R : set of raw data set
  - I : set of structured data set

$$T : R \longrightarrow I$$

$$r \longmapsto i(a_1, a_2, \dots, a_n)$$



- Necessary condition of a transformation function
  - ▶ The transformation function  $T$  must be rich
    - ◆ Without information loss that is useful to differentiate between the different connections
  - ▶ Poor function
    - ◆  $\exists$  connections that have
      - Different classes but
      - Same Attributes' values
  
- Reduce the number of incoherences for a precise learning

### ■ SNMPGUESS

- ▶ The connections of this class are not different from those of the normal traffic
- ▶ Due to the transformation function
  - The SNMP community passwords are not considered

### ■ SNMPGETATTACK

- ▶ Remains undetectable (password usurped)

### ■ Transformation tool DARPA 98 → KDD 99 unavailable

- ▶ Implementing a tool that transforms TCPdump traffic into well formed connections
  
- ▶ Slammer and the different DDoS tools (trino, etc.)
  - ◆ On-line network traffic transformation
  - ◆ On-line detection using decision trees
  - ◆ 100% of success classification as DoS attack type



1. Intrusion Detection
2. Motivations and New Attacks' Detection
3. Experimentation
4. Conclusion and Perspectives

## 4. Conclusion

---

- Improving the anomaly detection
  - ▶ New classes are considered
  - ▶ New attacks detection
  - ▶ Reduction of false positives ratio
  - ▶ Interesting results with KDD 99
- KDD 99 data sets critics
  - ▶ Necessary conditions for transformation are introduced
- Implementation
  - ▶ An on-line and off-line transformation and classification tools
  - ▶ Tests over real traffic

## 4. Perspectives

---

### ■ Hybrid alert correlation

- ▶ Improving the correlation techniques to consider this new anomaly technique

- Automatic extraction of attributes from the raw traffic
- Implementing the diagnosis methods
- Anticipating the detection before the end of the connection to launch on-line and real time counter measures

# Questions?

---

