

# Rules Based Network Anomaly Detection using Learning Automata

*Web mining project : IKT 407 module*

**Carry out by :**

*Ali Chelli  
Chen Leiming  
Farouk Dhahbi*

**Supervised by :**

*Prof. Ole-Christoffer  
Granmo*



# Plan

- Short initial summary
- Introduction, description of the plan work
- Literature survey and findings
- Problem statement
- Requirements, including requirements on  
how to verify results

# Short initial summary

- Learning automata is a new approach for the intrusion detection.
- Rules based network anomaly detection using learning automata
- implementation of the new method

# Introduction (1)

- Intrusion is an illegal action done by a network user.
- This action *might* be detrimental to the system, or to the service provided by the system.
- The denial of service attacks caused a loss of \$1.2 billion in the year 2000.

## Introduction (2)

- The main point is to evaluate the learning automata scheme for intrusion detection in computer network.
- Many automata will cooperate together in order to find a Boolean expression that can be used to decide whether the packet is normal or not.

# Learning Automata

- Learning Automata (LA) are adaptive decision making devices
- LA can operate in **unknown** and **non-deterministic** environment
- LA improve their performance by the means of a learning process

# Environment and Automaton Modelling

# *Learning Automata for anomaly detection*

# Planned work

- Get the packets from DARPA IDS
- Implement a program to be able to read the packets.
- Filter the packets
- Implementation of L A.
- Using L A in order to create new rules that will be used to decide whether the packet is normal or not.

# Literature survey and findings

- Network intrusion detection systems are classified as signature based or anomaly based.
- They both have their advantages and disadvantages.
- background material: <http://www.cs.fit.edu/~mmahoney/>
- paper or article reference : <http://www.cs.fit.edu/~mmahoney/paper6.pdf>
- filter programming : <http://www.cs.fit.edu/~mmahoney/dist/tf.cpp>
- DARPA IDS evaluation : <http://www.ll.mit.edu/IST/ideval/>

# Problem statement (1)

- Exploit the advantage of learning automata to develop a simple adaptive decision making program
- Can be used in the network as part of intrusion detection system
- Remove the suspicious traffic

# Problem statement (2)

- Principle



# Problem statement (3)



# Requirements

- <http://www.cs.fit.edu/~mmahoney/paper6>.
- Visual C++6
- Pcap library
- File contains packets
- Web page

Thank you for  
attention