Chapter 3 introduction to the IDS using fuzzy logic and grey theory

**3.1** Dataset

3.2 prediction engine

3.3 Detection model

3.4 Prediction Filter

3.5 Knowledge base

3.6 Model tuner

3.7 System Operator

3. 8 Summary

Chapter 4Construction of the system

4.1 Dataset Environment

4.1.1 Properties of the Dataset

4.2 Prediction Engine and Detection Model

4.2.1 Task Identification

4.2.2 Rule Evaluation

4.2.3 Properties of the content

**4.3** representation of the Knowledge base with fuzzy and grey

4.3.1 Knowledge concept relation representation

4.3.2 Knowledge concept Difficulty

4.3.3 Rule Evaluation

**4.4** Prediction Filter Concept based on fuzzy and grey theories

4.4.1 Structure of the prediction Filter

4.4.2 Properties of the prediction Filter

4.4.3 Agents and Environment of the prediction filter

4.4.4 specification of the prediction filter

4.5 Tuner model with controllers based on fuzzy and grey models

4.5.1 Task identification

4.5.2 Properties of the model tuner

4.5.3 Structure of the model tuner

4.6 Summary

Chapter 5 FUGRID System Implementation

5.1 Summary

Chapter 6 Experiments Results and Analysis

6.1 Experimental Design

6.2 Experimental Procedure

6.3 Measuring Instruments

6.4 Results

6.4.1 Rule Performance of IDS without tuning compared to some existing system

6.4.2 Comparison Performance of the rules tuned in FUGRID with the performance of these rules tuned in existing IDS without tuning

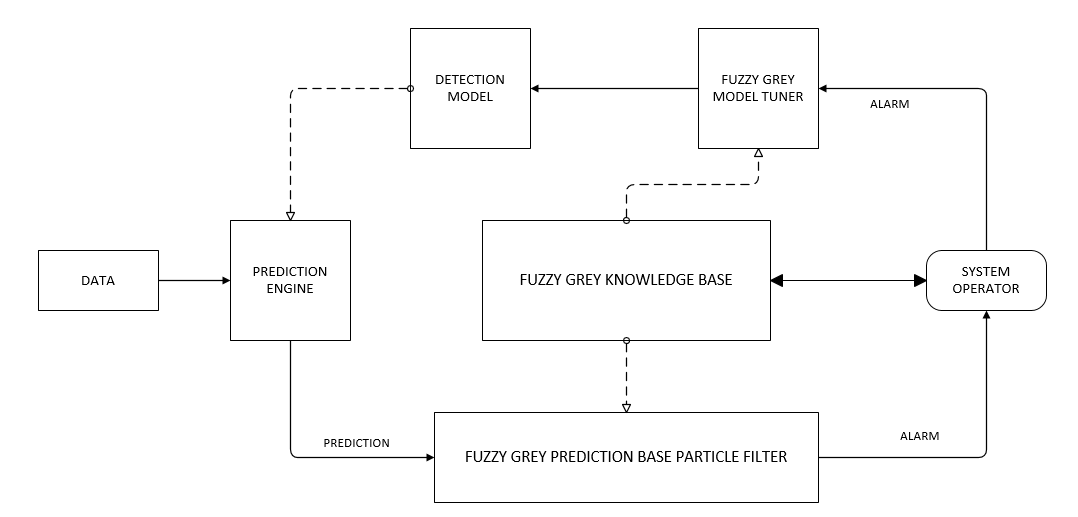
6.4.3 Comparison performance of some rules with high false rates with FUGRID with these high false rates tuned in existing IDS without tuning

6.4.4 Tuning observed in the experiment: number of rules tuned vs. number of predictions

triggering tuning and tuning strength vs. predictions triggering tuning with this or lower

strength.

This is my proposed FUGRID system



**The Research Scheme to be taken**

**The improved automated model tuner based on fuzzy logic and grey theory**

In the scheme of our model we aim to present an improved robust automated tuning intrusion detection system, which will aim to control the number of alarms output to the system operator and will tune the detection model adaptively according to responds sent by the system operator as and when false predictions are diagnosed.

The system will aim to revise its behavior

* by controlling the volume of alarms output to the operator in response to the competence of the operator to respond to these alarms to ensure system information security, and
* by deciding how frequently the detection model has to be tuned based on the accuracy of previous predictions.
  1. **Prediction Filter based on Fuzzy Logic and Grey Prediction**

Prediction filters are essential tools in modern science. They perform state prediction and parameter estimation in fields such as robotics, computer vision, and computer graphics. Sometimes also called Bayesian filters, they apply the Bayesian rule of conditional probability to combine a predicted behavior with some corrupted indirect observation. Predictive filters are a family of estimation techniques. They combine the uncertain prediction from the system’s dynamics and the corrupted observation. There are many different predictive filters, each dealing with different types of mathematical representations for random variables and system dynamics. A prediction filter in intrusion detection is used to forward only the most suspicious predictions to the system operator to be examined. The extent of predictions is regulated corresponding to the operator’s capability to respond to predictions to be verified in order to avoid overwhelming the system operator. Second, the system tunes the detection model when false predictions are identified and adjusts the tuning strength based on monitoring the performance of the detection model on earlier data.

In our work, we aim to present an improved prediction filter in an automated tuning intrusion detection system. To capture the sensitivity of these algorithms to individual system operators and to system history, the prediction filter we will propose will be based on Fuzzy Logic and Grey Theory

**4.3. An improved robust automated tuning IDS based on fuzzy logic and grey theory knowledge base**

Traditional intrusion detection mostly relies on the imperative knowledge of security experts, in particular, on their familiarity with the computer system to be protected. To reduce this dependence, various data-mining and machine learning techniques have been used in research projects.

The knowledge base we will adopt will be based on the Fuzzy Logic and Grey theory. The definitions of fuzzy sets, fuzzy rules are grey systems will be stored in a knowledge base and can be viewed and updated through a graphical user interface while the system is running. The user can change the function by setting new parameters. Our model aims to take advantage of the scrutiny of alarms by the system operators: the detection model will be tuned adaptively with the examined data with the objective of minimizing the workload on the system operator.