Annual review November 2013

Multi Metric Approach

Context

Systems of Systems and Industrial Contros Systems (ICSs)

- Searching for solutions for security interoperability in a systems of systems approach
- Metric will be always business oriented and therefore particularised to scenarios
  - Different metrics and diverse units
  - Indicators
- Operators need applicable tools for managing SPD measurement and always linked to business and operation
- We need to measure also the impact of SPD implementation and deployment in operation

Concept description

A Meta-heuristically Optimized Fuzzy Approach towards Multi-Metric Security Risk Assessment in Heterogeneous System of Systems

- Risk based metrics identification
- Fuzzy expert system for aggregation and composition (if-then-else clauses): for operator comprehension
- Meta-heuristic (genetic algorithms) for metric precision and accuracy mechanism as learning system

Easy to design and understand by operator/end user

Subjectivity is based on the knowledge of the operator

nSHIELD

Steps

We need the following steps for managing SMART SECURITY metrics:

- **Scenario risk analysis and risk identification:** examples 1) delay 2) man in the middle
- **Selection of metrics:** system operators will select specific security metrics according to the requirements and risk factors of the scenario at hand. (more than 60 in 2.5)
  - Example for risk identified:
    - Network latency
    - Key length for simetric algorithm

- **Normalization and regression:** Each of the metrics identified previously may feature different units and value range. Example Network Latency:
  - Finally we get a SPD metric: e.g. M_{NL} = [20, 40, 60]

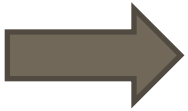
Network Latency Metric

Time	0	1	2	3	4	5	6	7	8	9	10	11	15	25
S-Level	0	2	4	6	8	11	14	17	20	23	26	32	44	58

Steps

- **Fuzzy System as understandable mechanisms for operators and scenario owners**:
  - Develop linguistic fuzzy variables

Linguistic Variables for INPUTS in ES	Fuzzy [SPD] triangular
Very Low	[0,0,1]
Low	[10,15,18]
Medium	[30, 40, 26]
Medium-High	[60, 55, 66]
High	[80,75,88]



Linguistic Variables for OUTPUTS in ES
Green
Red
Yellow

Steps

- **Fuzzy Expert Systems** : Consists of an aggregation and decision making engine that processes the numerical values of the monitored security metrics
  - With IF-THEN-ELSE conditional statements we get composition
  - Tailor the mapping between the numerical and linguistic domains corresponding to the SPD values of the considered metric with their fuzzy representation and processing through the rule set

IF S_{NL} is HIGH and D_{KeyMan} is MEDIUM-HIGH
then
Matrix [Network, S] := Green
IF ….

Steps

- **Meta-heuristically LEARNING system optimisation**
  - An Outcome example from expert system could be as follows

	S	P	D
Node	G	R	R
Network	Y	Y	Y
Middleware	Y	G	R
Overlay	G	Y	Y

  - However system operator could decide depending his/her experience that the correct systems status is:

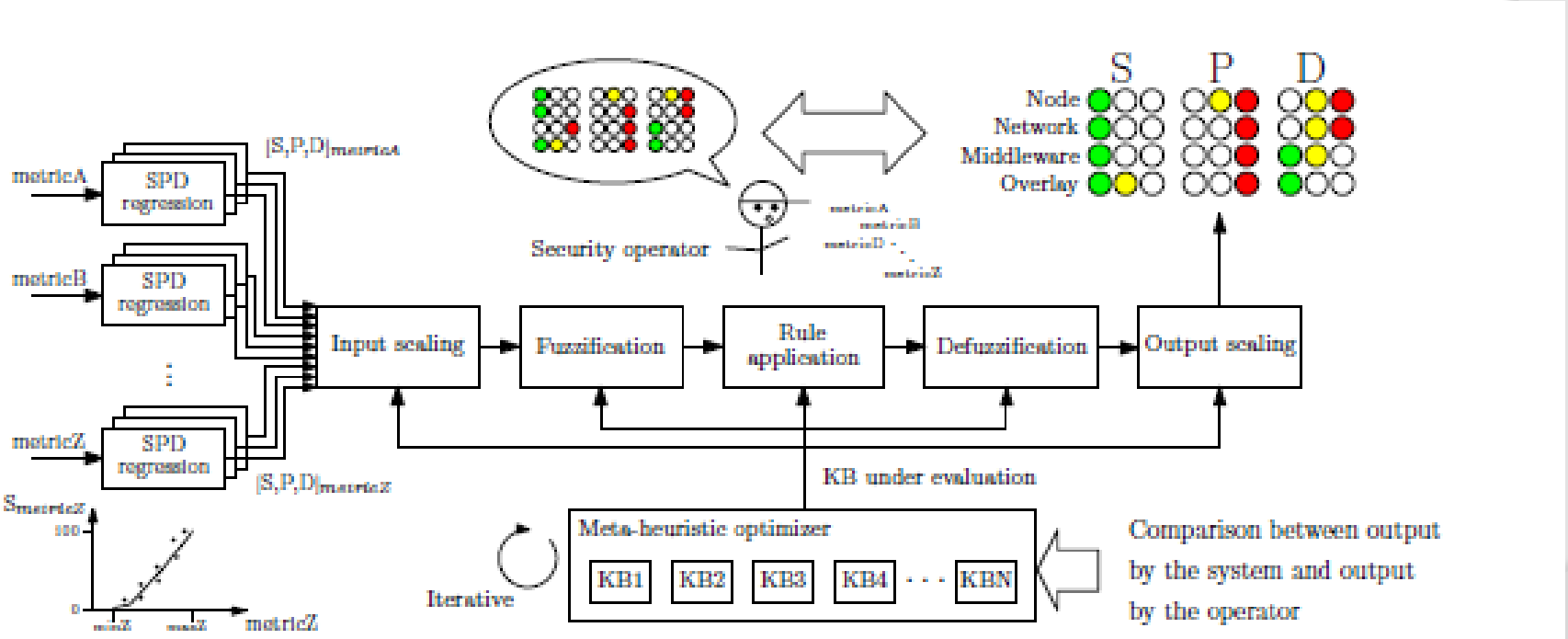
	S	P	D
Node	G	R	R
Network	Y	Y	Y
Middleware	Y	G	Y
Overlay	G	Y	Y

  - Via evolutionary algorithms, we plan to analyze and benchmark the performance. As optimiser metric we will use:
    Optimiser metric = nº of correct colours / nº of total colours
  - For new members for evolutionary iteration mutation will be solved:
    1. changing linguistic variables and SPD table
    2. Changing expert system inference rules according to expert system

nSHIELD

Steps

- Multi-metric Aggregation based on Expert Systems and Meta-heuristically Optimized Fuzzy Systems. Architecture.



Implementation

1) We are approaching the implementation through an extension of an agent developed by TUC
2) Event Calculus to formally model the dynamic behavior of multi-metric approach
3) Considering cost concept to have an economic assessment for decision making
4) This is an ongoing task

The END

That’s all folks!