Semantic Models for Network Intrusion Detection

Peter Bednár, Martin Sarnovský, Pavol Halas
Technical University of Kosice

Eclipse SAM IoT 2020
Security | AI | Modelling

Supported by: BRAIN-IoT

Photo by Josh Riemer on Unsplash

Intrusion Detection Systems

- two main approaches for IDS:

- **knowledge oriented** – manually crafted rules for detection of intrusions or for the modelling of the normal behavior
- **data oriented** – application of machine learning methods
  - classification, anomaly detection
  - unbalanced datasets

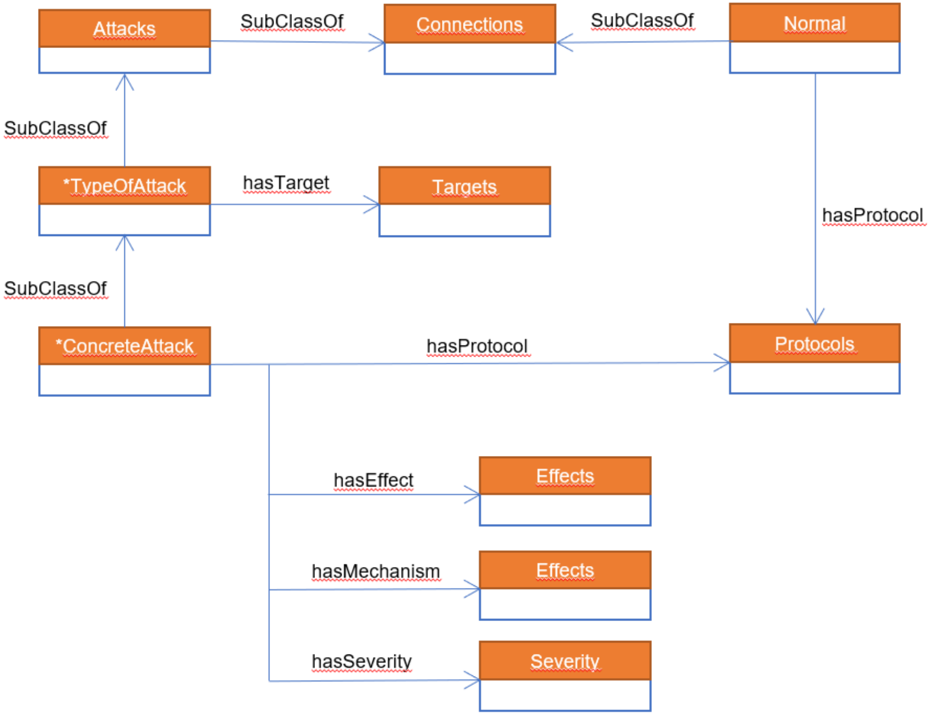
Combined approach

- Formalize data in the form of semantic model – ontology
- Use domain knowledge to overcome problems of statistical inference in machine learning
    - Problem decomposition
    - Minor classes can be detected by formalized rules
    - But also use explainable AI to enhance knowledge model

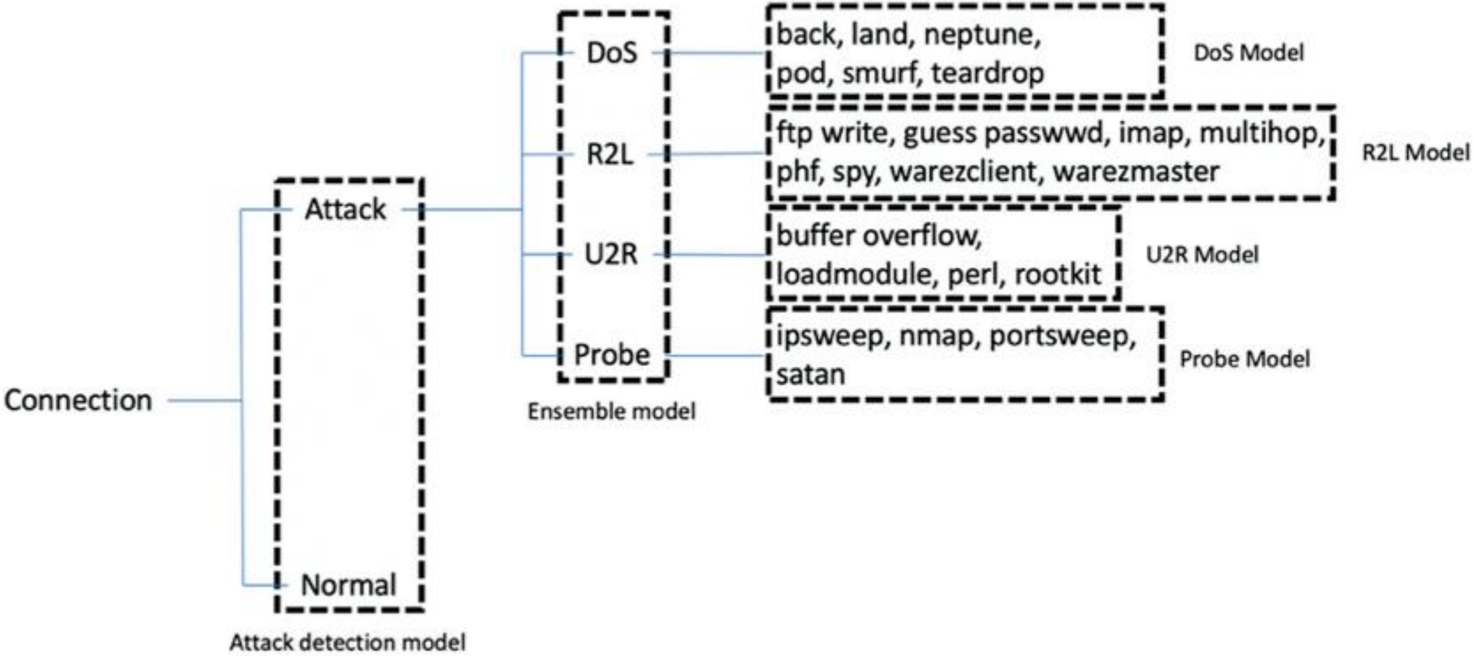
Network Intrusion Ontology

- Taxonomy of intrusion types
- Data properties and relations describing:
    - Connections, Flags, Protocols, Targets
    - Mechanisms
    - Effects, Severities
    - Targets

Core concepts of the semantic model



Hierarchical classification schema



Evaluation

- KDD Cup 99 dataset

- standard benchmark for network IDS
- 22 types of the attacks, 33 features
  - Mapped to the ontology model

Experiment results (1)

	Normal	Attack	Precision	Recall
Normal	29,095	11	0.999	0.999
Attack	35	119,066		

Experiment results (2)

	Probe	U2R	DoS	R2L	Prec.	Rec.
Probe	1279	0	1	0	0.992	0.992
U2R	0	15	0	0	1	0.882
DoS	6	0	117,385	0	0.999	0.999
R2L	4	2	0	331	0.982	1

Experiment results (3)

Classifier	Acc.	Prec.	F1	FAR
C4.5	0.969	0.947	0.970	0.005
Random forests	0.964	0.998	0.986	0.025
Forest PA	0.975	0.998	0.998	0.002
Ensemble model	0.976	0.998	0.998	0.001
Our approach	**0.998**	**0.998**	**0.998**	0.001

Conclusions

- Sinergy between knowledge-based and data-based models

- Explore more relations in the data
- Explainable AI to enhance knowledge model
  - Automatically formalize cases