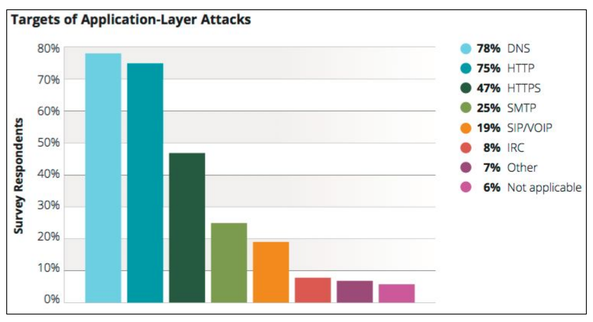
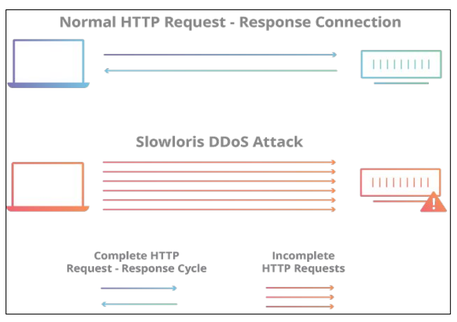
Ontology Based Intrusion Detection System

Aarti Kashyap, Akshay Gopalakrishnan
kaarti.sr@gmail.com, akshayg95@gmail.com
University of British Columbia, McGill University

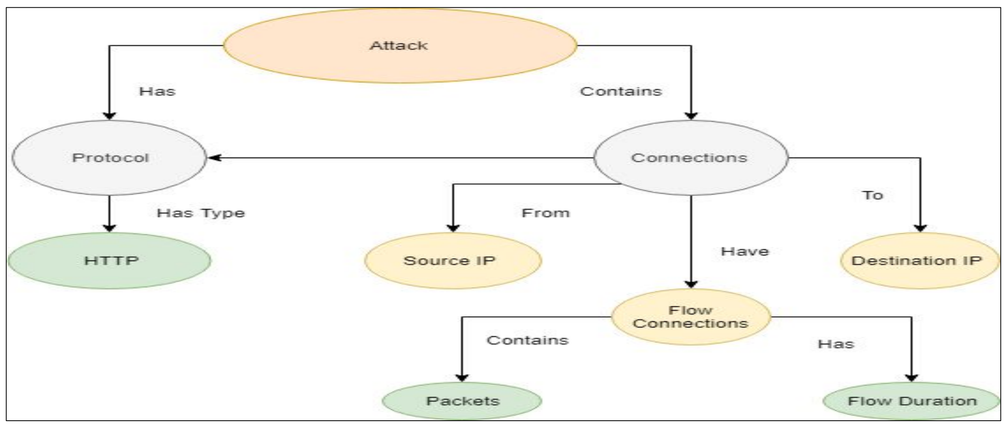
Motivation

- Increasing number Network-based attacks
- New DDOS attacks: Slow-DOS, Slowloris, Slow-Read[3]
- No generalized means to detect attacks on HTTP layer
- Ontology based approach provides right means to generalize the different attacks.

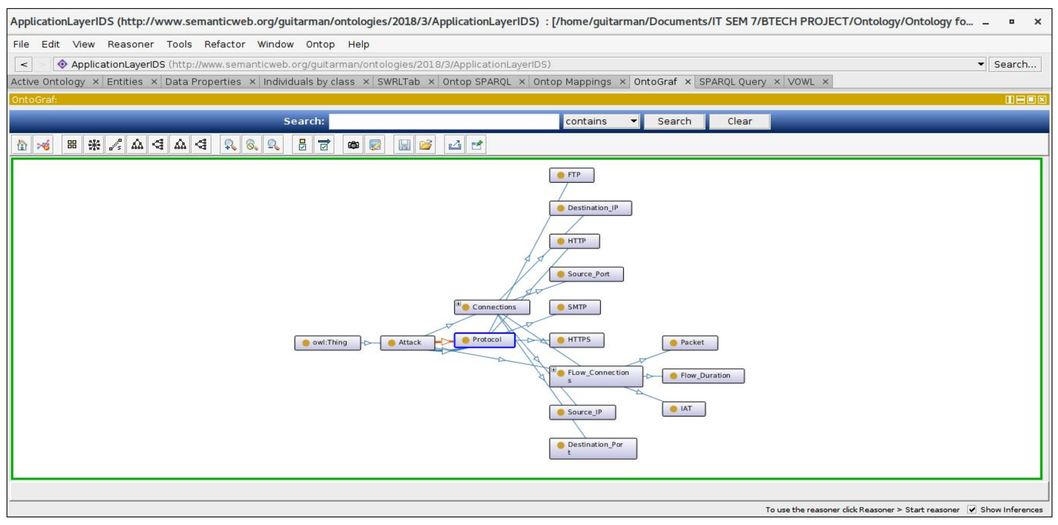




HTTP Attack Ontology



- A high level view of our Ontology is given on the left. The ontology is based on our concept of what an attack network connection would have.

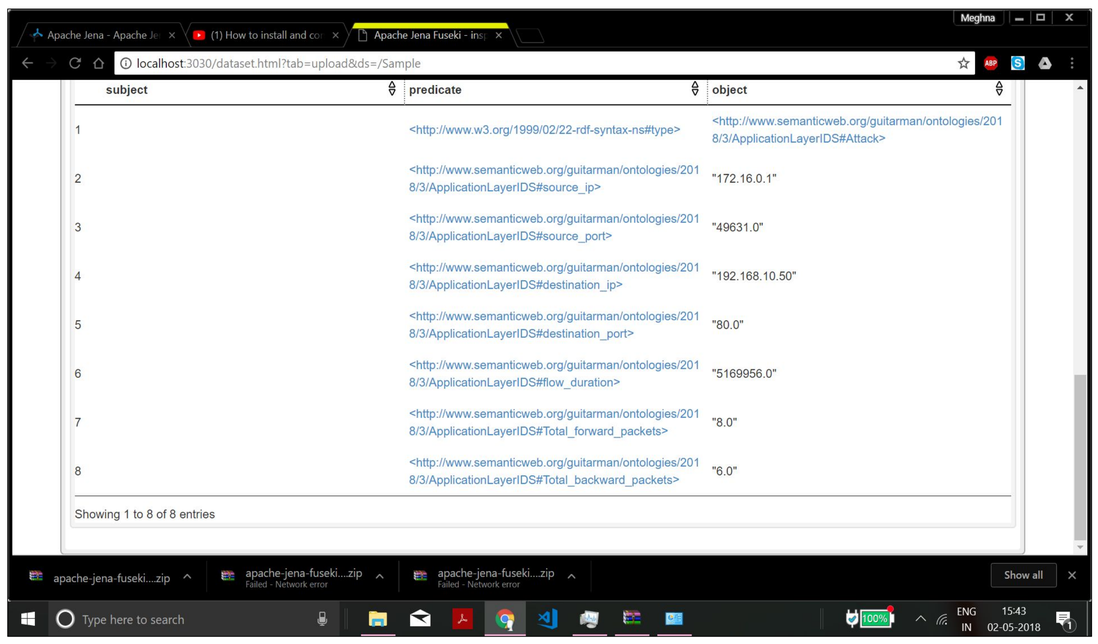


- The concept is then concretized using the tool Protege which is used to build Ontologies.

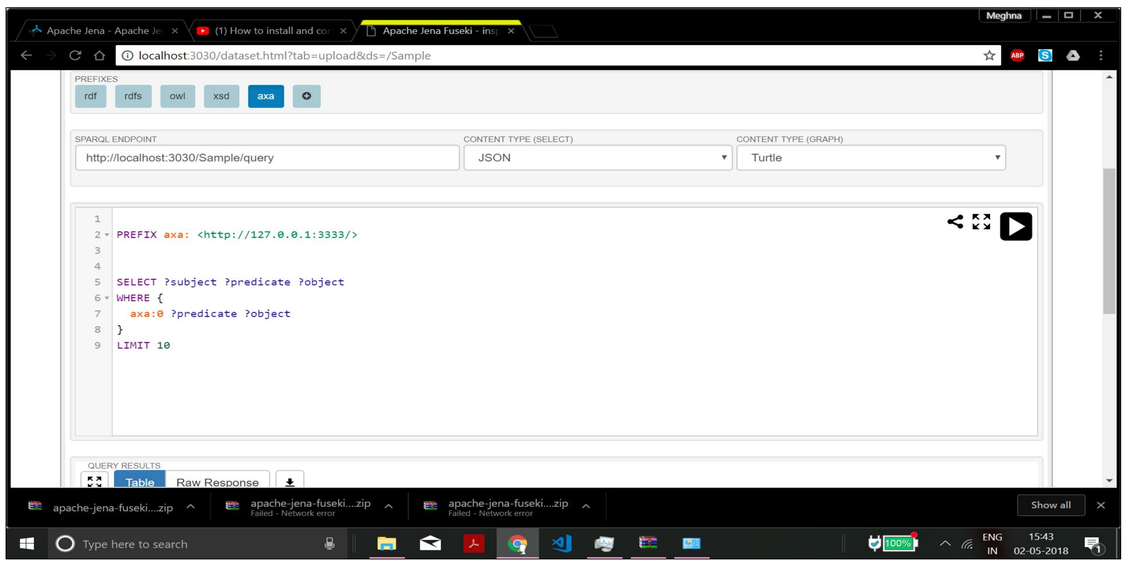
Advantages of Ontology

- Ontology is general but the queries can be constructed for specificity.
- Ontology gives us the ability to build a generalised system and not just for one specific attack.
- The same network ontology can be extended and used in other domains to detect network attacks.

Querying the Ontology



- The above figure shows a partial result of a query asking to show all the information stored in the ontology.
- We use such queries to fetch us information from the ontology that might help us detect an attack



- The information is stored using our ontology and we retrieve information about connections from the ontology using SPARQL Queries.

Tools/Datasets

- Ontology construction and queries: Protege[1], GoogleRefine/OpenRefine [2], Apache Jena Fuseki [5]
- Data set: CICIDS2017 [4]

Discussions/Future Work

- Extend and reuse network ontology for different systems to show generalisability.
- Extend it to construct entire system ontology with network as one component.

Bibliography

1. https://protege.stanford.edu/
2. http://openrefine.org/download.html
3. https://blogs.akamai.com/2013/09/slow-dos-on-the-rise.html
4. Iman Sharafaldin, Arash Habibi Lashkari and Ali A. Ghorbani, “Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization”
5. https://jena.apache.org/documentation/fuseki2/