Improving Protocol Vulnerability Discovery via Semantic Interpretation of Textual Specifications
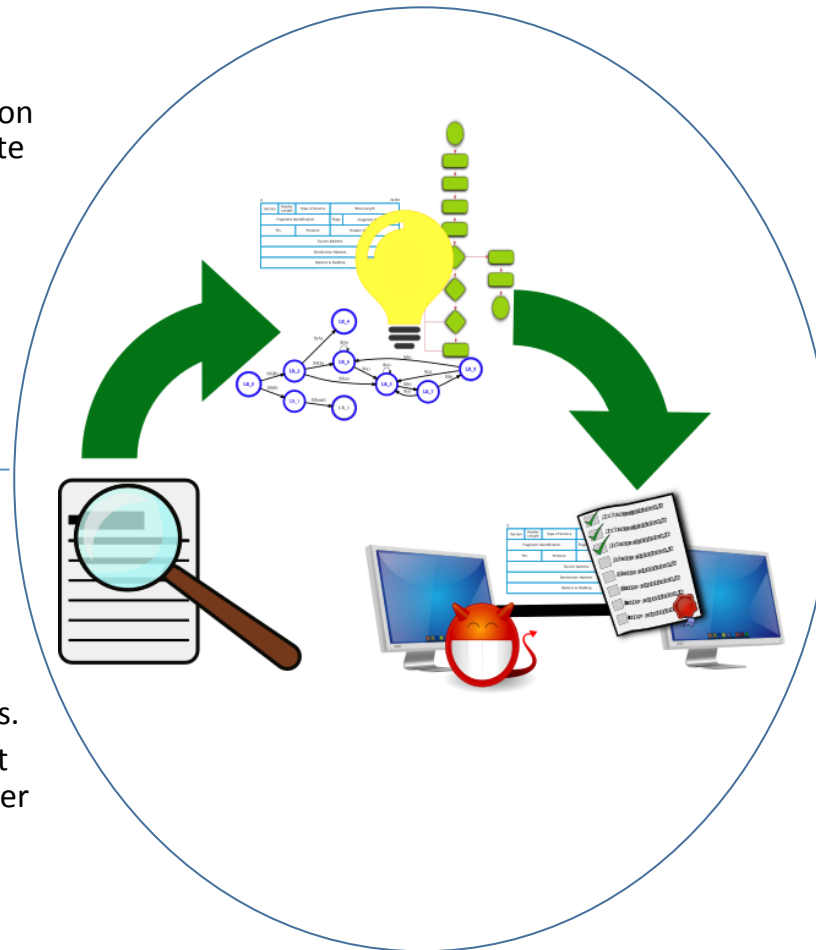

Challenge:

- Network protocol testing requires structured information such as message formats, state machine, constraints, etc.
- Such information is derived manually by people with different levels of expertise, and represents a challenging, time consuming and error-prone task.

Scientific Impact:

- Completely automate testing and model checking of network protocols.
- Allow for new design methodologies, implementation and testing, impacting fields beyond networking.

Solution:

- Extract structured information from protocol documents using semantic interpretation NLP techniques.
- Validate our approach against RFCs, Internet drafts, and other standard documents.

Broader Impact:

- Contribute to obtaining increased assurance in protocol design and implementation (Internet, IoT, wireless).
- Create a repository with all the extracted structured information for protocols and make it available to the research community.