Poster: Semantic Modelling of DDoS Attacks: An Ontology-Driven Cybersecurity Framework

Durre Zehra Syeda
School of Computer Science,
College of Science and Engineering
University of Galway
Galway, Ireland
d.syeda1@universityofgalway.ie

Mamoona Naveed Asghar
School of Computer Science,
College of Science and Engineering
University of Galway
Galway, Ireland
mamoona.asghar@universityofgalway.ie

***Abstract*—**
This research proposes a domain-specific ontology for Distributed Denial of Service (DDoS) attacks, developed using Web Ontology Language (OWL) and Protégé, to overcome the limitations of conventional detection approaches that lack semantic awareness and structured knowledge representation. Unlike purely data-driven methods, the proposed ontology formalises key concepts, relationships, and behaviours associated with exploitation- and reflection-based DDoS attacks, enabling a richer contextual understanding of threat patterns. This structured semantic framework supports integration with threat intelligence platforms and facilitates automated reasoning, providing a foundation for more informed and interpretable machine learning (ML) models. By embedding ontological knowledge into the deep learning (DL) pipeline, the approach aims to enhance detection performance, improve model explainability with the usage of explainable AI (XAI), and support timely and adaptive responses to evolving DDoS threats.

***Index Terms*—DDoS attacks, DDOS Exploitation Attacks, DDoS Reflection Attacks, Knowledge Representation, Ontology-Driven Detection, Machine Learning, Deep Learning, Explainable AI**

I. Introduction

DDoS attacks pose a persistent threat to online services, causing severe disruptions and financial losses (Hai et al. [1]; Owusu et al. [2]). Their growing complexity demands intelligent, real-time detection mechanisms (Singh et al. [3]). Ontology enables semantic representation of DDoS attack patterns (Haddadi et al. [4]), behaviours, and relationships, which improves detection accuracy, contextual reasoning, and interoperability across cybersecurity systems. This research proposes a novel, ontology-driven framework to address this challenge. Developed in OWL [1] using Protégé[2], the ontology models a detailed vocabulary of exploitation and reflection-based DDoS attacks. It enhances semantic understanding and interoperability with threat intelligence systems, providing a foundation for reasoning-based analysis (Lin & Tseng [5]). Additionally, it will support the development of DL and XAI models by embedding attack context into training data (Rajan et al. [6]; Su et al. [7]; Chaganti et al. [8]). It will also focus on the integration and modelling relationships of real-world datasets among attack vectors, vulnerabilities, and mitigations (AlJuhani et al. [9]; Pokrinchak et al. [10]; Kuadey et al. [11]).

Literature Review: Table I highlights recent contributions to DDoS research, with a focus on ontology, DL models, XAI and dataset generation. While existing studies often address individual components, our research uniquely integrates all these elements into a unified framework.

TABLE I
Comparison of Related Work with our Research. (Ont: Ontology), (XAI: Explainable AI), (DG: Dataset Generation), (NA: Not Applicable), (HTTP: Hypertext Transfer Protocol)

Existing Research	DDoS	Ont	DL	XAI	DG
Haddadi 2025 [4]	HTTP	✓	✗	✗	✗
Ayo 2024 [12]	NA	✓	✓	✗	✗
Hnamte 2024 [13]	SDN	✗	✓	✗	✗
Alashhab 2024 [14]	SDN	✗	✓	✗	✗
Our Research	All	✓	✓	✓	✓

Research Gap: Table I shows that existing ML/DL approaches to DDoS detection often lack semantic context and fail to represent the hierarchical and behavioural characteristics of attacks. The limited use of ontologies has led to gaps in explainability, standardisation, and integration with threat intelligence. Our solution addresses these limitations by introducing a structured, knowledge-driven ontology to enhance contextual understanding, support reasoning, and improve the interpretability of detection systems.

Research Objectives: Based on the identified research gap, our research aims to answer the following four research objectives (ROs):

RO1: Design and develop a domain-specific ontology to formally represent key DDoS characteristics, i.e. protocol type, packet size, flow duration, and attack vector.

RO2: Integrate the ontology with available datasets and real-time traffic for DL-based detection.

RO3: Train and evaluate DL models using ontology-enriched data to assess DDoS attack classification accuracy and performance improvements.

RO4: Enhance model explainability and generate an ontology-driven dataset for future research.

[1]https://www.w3.org/OWL/
[2]https://protege.stanford.edu/

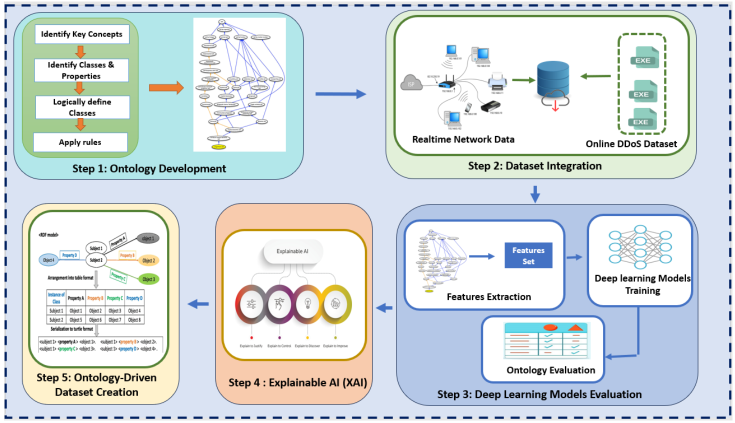

Fig. 1. An Ontology-driven Cybersecurity Framework for the analysis of DDOS attacks (development, training and evaluation)

Research Contributions: Through the pursuit of given ROs, this study will provide following contributions:

- ***Semantic Enrichment:*** A domain-specific OWL-based ontology capturing attack types, symptoms, behaviours and mitigations. Adds a knowledge layer to existing detection systems to improve context reasoning.
- ***Explainability:*** Increases transparency by semantically tagging ML inputs/outputs for better interpretability.
- ***Dataset Integration:*** Integrate with benchmark datasets (e.g., CIC-DDoS2019[3], UNSW-NB15[4]) to generate a new structured dataset with advanced semantic.

II. Methodology

The methodology adopted in Figure 1 follows five key stages, beginning with developing a domain-specific DDoS ontology that defines core concepts, classes, and relationships. Secondly, this ontology will be integrated with datasets and live traffic to enrich data semantically. The DL models will be trained and evaluated, followed by XAI techniques to enhance interpretability. Finally, generating an ontology-driven dataset to support future research in semantic-based intrusion detection. Figure 2 illustrates the developed DDoS ontology, detailing exploitation- and reflection-based attacks along with their subtypes. It captures static and dynamic behaviours, along with temporal aspects, offering a rich semantic model. It also facilitates a **real-world applications** like real-time attack detection, automated response, and threat analysis in **cloud services, ISPs, and smart city networks**.

III. Challanges

Key challenges include handling high-volume real-time data, reasoning scalability, evolving attack patterns, and seamless integration with AI models.

IV. Conclusion

This research presents a comprehensive ontology for DDoS attacks, providing a structured semantic framework to classify and analyse exploitation and reflection-based attack behaviours. Designed for extensibility, it supports integration with existing datasets and real-time systems, promoting standardisation and interoperability in DDoS research.

V. Limitation & Future Work

As this research is centred on ontology development, no empirical validation has yet been carried out using annotated datasets, DL models, or real-time systems. The practical utility of the ontology in live detection scenarios is yet to be established. **Future work** will involve generating a structured dataset from the ontology, integrating it with live traffic for real-time DDoS detection, and linking it with DL models to support semantic-based intrusion detection and explainability on decision-making. Model performance will be evaluated using metrics i.e. accuracy, precision, recall, and F1-score metrics.

Acknowledgment

This research is supported by Research Ireland Grant No. GOIPG/2024/4674.

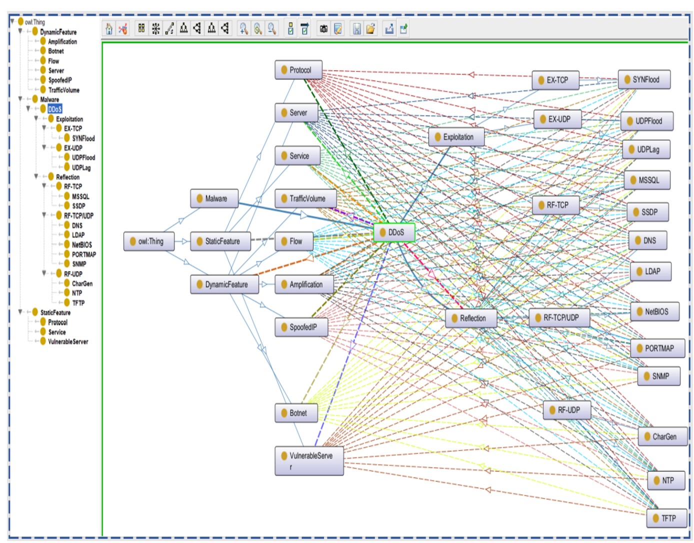

Fig. 2. Developed Ontology for DDoS attacks

[3]https://www.unb.ca/cic/datasets/ddos-2019.html
[4]https://research.unsw.edu.au/projects/unsw-nb15-dataset

REFERENCES

[1] T. H. Hai, N. T. Khiem, and N. H. Phuc, "Toward an online dos/ddos classification: An empirical study for network intrusion detection systems," *Journal of Computer Science*, vol. 17, no. 3, pp. 304–318, Mar 2021. [Online]. Available: https://thescipub.com/abstract/jcssp.2021.304.318

[2] E. Owusu, M. Rahouti, S. K. Jagatheesaperumal, K. Xiong, Y. Xin, L. Lu, and D. F. Hsu, "Online network dos/ddos detection: Sampling, change point detection, and machine learning methods," *IEEE Communications Surveys & Tutorials*, 2024.

[3] C. Singh and A. K. Jain, "A comprehensive survey on ddos attacks detection & mitigation in sdn-iot network," *e-Prime-Advances in Electrical Engineering, Electronics and Energy*, p. 100543, 2024.

[4] M. Haddadi, A. Khiat, H. Bouaoud, and H. Djehiche, "Spgdad: Slow http-get denial of service attack detection using ontology," *Information Security Journal: A Global Perspective*, vol. 34, no. 1, pp. 79–87, 2025.

[5] S.-C. Lin and S.-S. Tseng, "Constructing detection knowledge for ddos intrusion tolerance," *Expert Systems with Applications*, vol. 27, no. 3, pp. 379–390, 2004. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0957417404000417

[6] D. Rajan, "Quantum analogue of entropy based ddos detection," *arXiv preprint arXiv:2111.11867*, 2021.

[7] Y. Su, D. Xiong, K. Qian, and Y. Wang, "A comprehensive survey of distributed denial of service detection and mitigation technologies in software-defined network," *Electronics*, vol. 13, no. 4, p. 807, 2024.

[8] R. Chaganti, R. V. Boppana, V. Ravi, K. Munir, M. Almutairi, F. Rustam, E. Lee, and I. Ashraf, "A comprehensive review of denial of service attacks in blockchain ecosystem and open challenges," *IEEE Access*, vol. 10, pp. 96 538–96 555, 2022.

[9] A. Aljuhani, "Machine learning approaches for combating distributed denial of service attacks in modern networking environments," *IEEE Access*, vol. 9, pp. 42 236–42 264, 2021.

[10] M. Pokrinchak and M. M. Chowdhury, "Distributed denial of service: Problems and solutions," in *2021 IEEE International Conference on Electro Information Technology (EIT)*. IEEE, 2021, pp. 032–037.

[11] N. A. E. Kuadey, G. T. Maale, T. Kwantwi, G. Sun, and G. Liu, "Deepsecure: Detection of distributed denial of service attacks on 5g network slicing—deep learning approach," *IEEE Wireless Communications Letters*, vol. 11, no. 3, pp. 488–492, 2021.

[12] F. E. Ayo, J. B. Awotunde, L. A. Ogundele, O. O. Solanke, B. Brahma, R. Panigrahi, and A. K. Bhoi, "Ontology-based layered rule-based network intrusion detection system for cybercrimes detection," *Knowledge and Information Systems*, vol. 66, no. 6, pp. 3355–3392, 2024.

[13] V. Hnamte, A. A. Najar, H. Nhung-Nguyen, J. Hussain, and M. N. Sugali, "Ddos attack detection and mitigation using deep neural network in sdn environment," *Computers & Security*, vol. 138, p. 103661, 2024.

[14] A. A. Alashhab, M. S. Zahid, B. Isyaku, A. A. Elnour, W. Nagmeldin, A. Abdelmaboud, T. A. A. Abdullah, and U. D. Maiwada, "Enhancing ddos attack detection and mitigation in sdn using an ensemble online machine learning model," *IEEE access*, vol. 12, pp. 51 630–51 649, 2024.

Semantic Modelling of DDoS Attacks: An Ontology-Driven Cybersecurity Framework

Durre Zehra Syeda [1] Mamoona Naveed Asghar [2]

School of Computer Science, College of Science and Engineering, University of Galway, Ireland

Abstract

This research proposes a domain-specific ontology for Distributed Denial of Service (DDoS) attacks, developed using Web Ontology Language (OWL) and Protégé, to overcome the limitations of conventional detection approaches that lack semantic awareness and structured knowledge representation. Unlike purely data-driven methods, the proposed ontology formalises key concepts, relationships, and behaviours associated with exploitation and reflection-based DDoS attacks to enable a richer contextual understanding of threat patterns. This structured semantic framework supports integration with threat intelligence platforms and facilitates automated reasoning to provide a foundation for more informed and interpretable Machine learning (ML) models. The approach aims to enhance detection performance, improve model explainability using explainable AI (XAI), and support timely and adaptive responses to evolving DDoS threats by embedding ontological knowledge into the Deep learning (DL) pipeline.

Keywords: DDoS attacks, DDOS Exploitation Attacks, DDoS Reflection Attacks, Knowledge Representation, Ontology-Driven Detection, Machine Learning, Deep Learning, Explainable AI

Introduction

DDoS attacks pose a persistent threat to online services, causing severe disruptions and financial losses. **Ontology** enables semantic representation of DDoS attack patterns, behaviours, and relationships, which improves detection accuracy, contextual reasoning, and interoperability across cybersecurity systems. This research proposes a novel, ontology-driven framework developed in OWL[a] using Protégé[b] to address this challenge. The ontology models a detailed vocabulary of exploitation and reflection-based DDoS attacks and addresses the lack of semantic structure in traditional detection methods. This approach aims to improve detection accuracy, model explainability, and real-time response to evolving DDoS threats.

Literature Review

Table 1 highlights recent contributions to DDoS research, with a focus on ontology development, DL models, XAI and dataset generation. While existing studies often address individual components, our research uniquely integrates all these elements into a unified framework.

Table 1. Related Work on DDoS Attack VS our Research. (XAI: Explainable AI), (DG: Dataset Generation), (SB: Static Behaviour), (DB: Dynamic Behaviour), (NA: Not Applicable), (HTTP: Hypertext Transfer Protocol)

Existing Researches	DDoS	Ontology	Deep Learning	XAI	DG	SB	DB
Alashhab 2024 [1]	SDN	✗	✓	✗	✗	✗	✗
Ayo 2024 [2]	NA	✓	✓	✗	✗	✗	✗
Gowripeddi 2023 [3]	NA	✓	✗	✗	✗	✗	✗
Haddadi 2025 [4]	HTTP Flood	✓	✗	✗	✗	✗	✗
Our Research	All types	✓	✓	✓	✓	✓	✓

Research Gap: Current DL-based DDoS detection methods lack semantic context and fail to capture the hierarchy and behaviour of attacks. This research introduces a structured ontology to enhance contextual understanding & reasoning, improve prediction & explainability and interpretability of detection systems.

Research Objectives

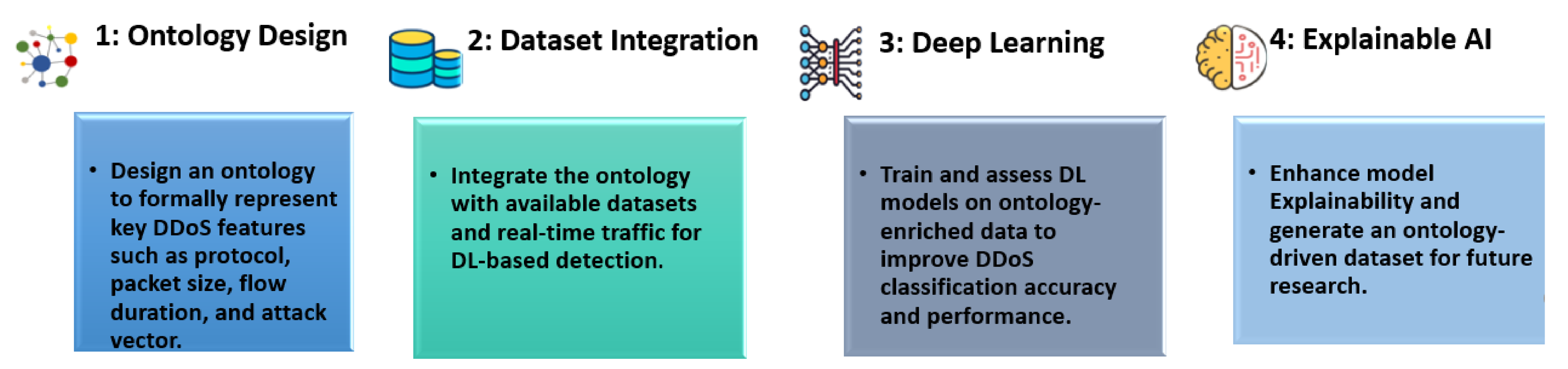

Figure 1. Based on the identified research gap, our research aims to answer the following four research objectives

Research Contributions

The contributions of this study are as follows:

- **Semantic Enrichment:** An ontology capturing DDoS attack types, behaviours, and mitigations.
- **DL Integration:** Enhances intelligent threat prediction by integrating DL-Models .
- **Explainability :** Boosts transparency by semantically tagging ML inputs/outputs.
- **Dataset Integration:** Integration with baseline datasets to supports real-time traffic monitoring.

Real-world Applications Use cases

Domain	Application of DDoS Ontology
Cloud Service	Real-time DDoS classification and mitigation (e.g., AWS, Azure).
Smart City	Securing IoT-enabled systems from coordinated botnet attacks.
Financial Institutions	Temporal threat correlation and incident response.
Security Operations Centers	Context-aware dashboards and forensic threat analysis.

Methodology

Our research methodology, outlined in **Figure 2**, comprises **five key stages**.

- **Step 1:** Developing a domain-specific DDoS ontology, defining concepts, classes, and relationships.
- **Step 2:** Integrate into datasets and real-time traffic to enrich attack data with semantic context.
- **Step 3:** Training and evaluation of DL models on this enhanced data.
- **Step 4:** Application of XAI techniques to improve interoperability.
- **Step 5:** Generate an ontology-driven dataset to support future research.

[a] https://www.w3.org/OWL/
[b] https://protege.stanford.edu/

Conceptual Framework

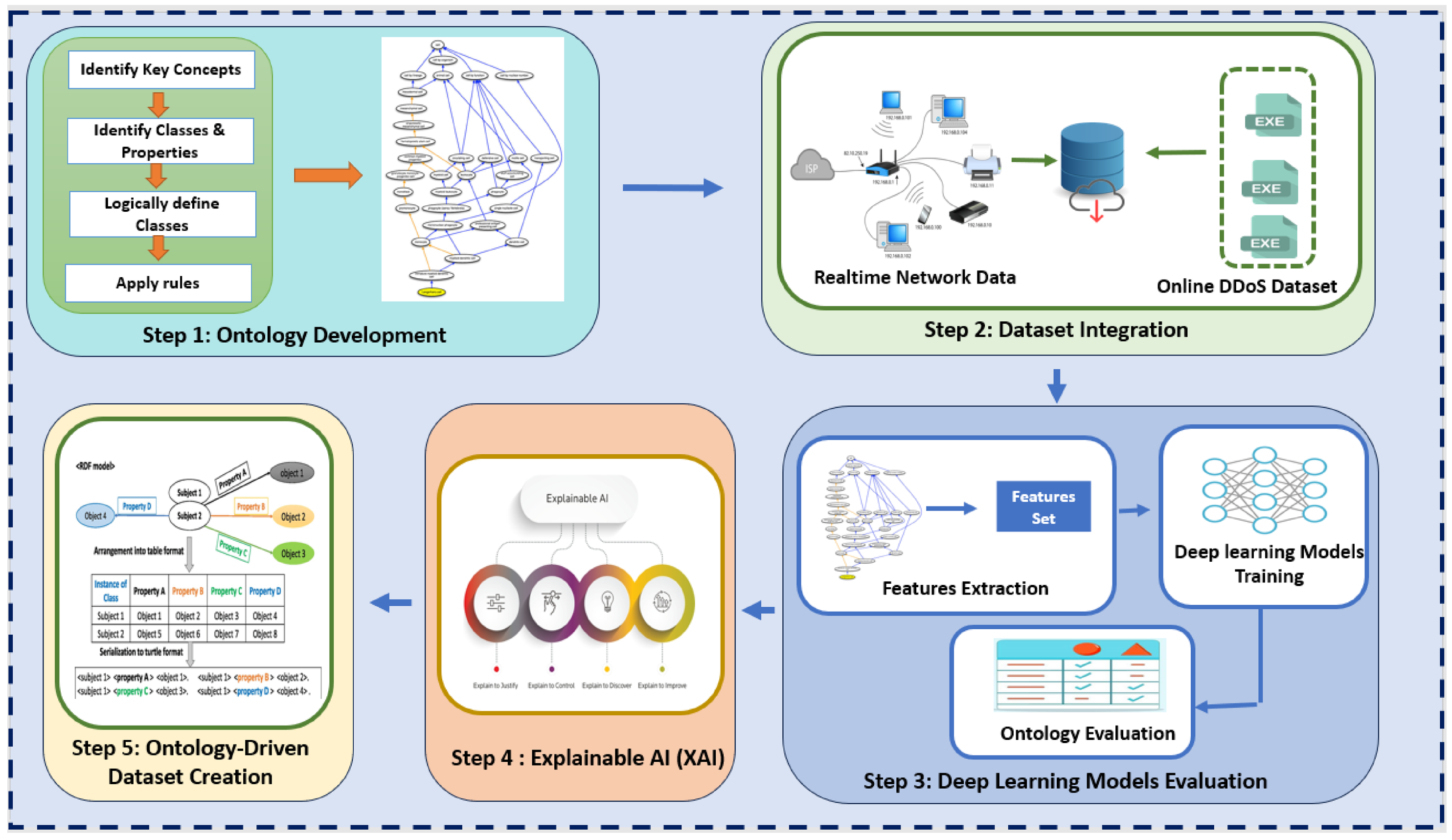

Figure 2. An Ontology-driven Cybersecurity Framework for the analysis of DDOS attacks (development, training and evaluation)

DDoS Ontology

Figure 3 illustrates the DDoS ontology structure, outlining two main attack categories: Exploitation and Reflection, along with their subtypes. It integrates static features (e.g., protocols) and dynamic behaviours (e.g., traffic patterns), providing a semantic framework for enhanced detection and reasoning. **Time-Dependent Concepts** like `AttackTimestamp`, `AttackDuration`, `FirstObserved`, `LastObserved`, and `EvolutionStage` will be used to capture temporal aspects of DDoS behaviour.

DDoS Ontology Visualization

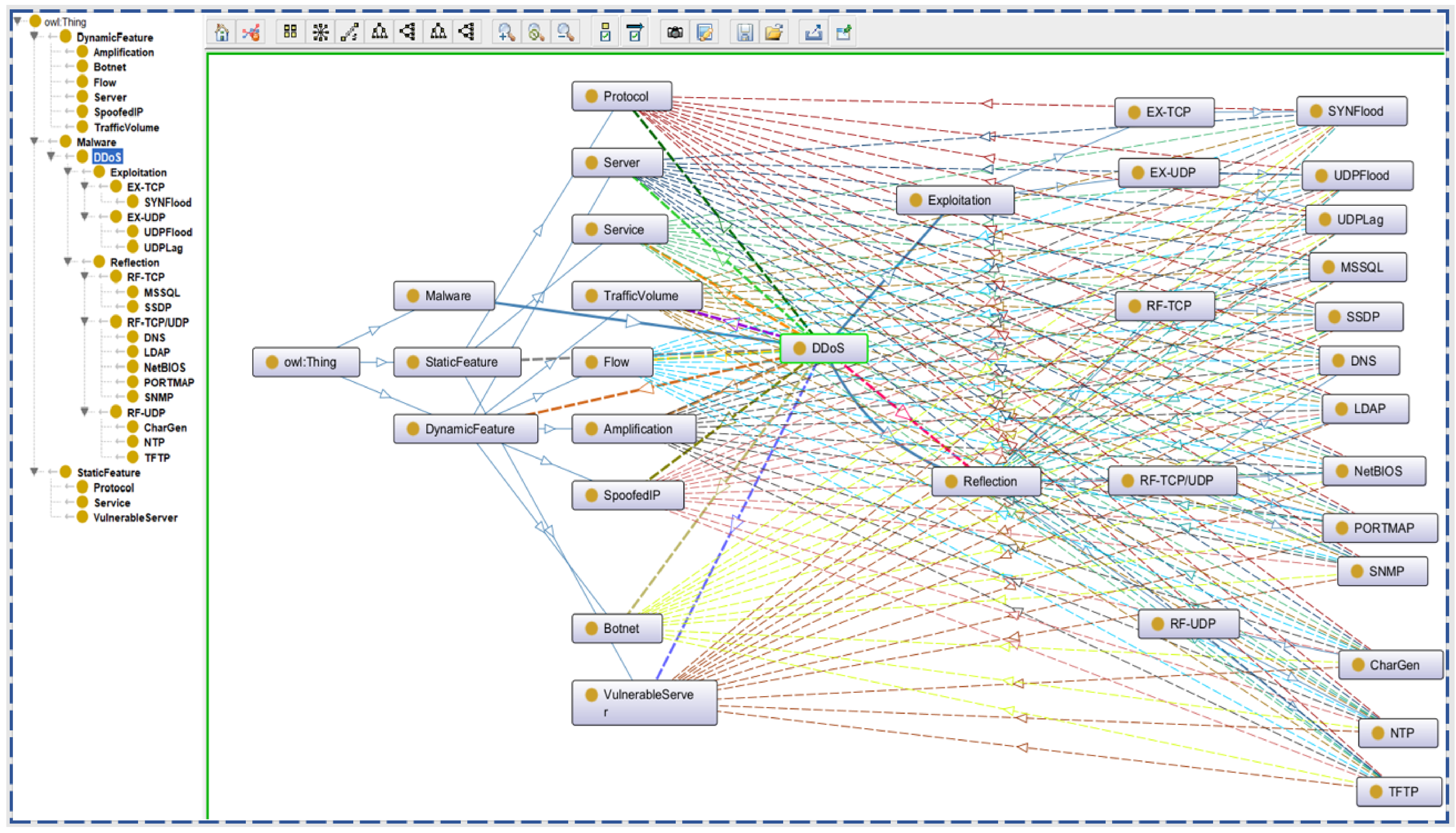

Figure 3. Developed Ontology for DDoS attacks (Data Visualization)

Challenges - Scalability issues and Solutions for DDoS Ontology

Challenges	Mitigation Strategy
High data volume	Use modular ontology design.
Ontology reasoning overhead	Use lightweight or rule-based reasoning.
Evolving attack patterns	Design an extensible ontology.
</> Integration with AI models	Preprocess ontology context into ML features.

Conclusion

The developed ontology provides a semantic framework for the semantic representation of DDoS attack patterns, behaviours, and relationships. This improves detection accuracy, contextual reasoning, and interoperability across cybersecurity systems while supporting integration with datasets and real-time systems for standardised, extensible cybersecurity research.

Limitation & Future Directions

As this research is centred on ontology development, no empirical validation has yet been carried out using annotated datasets, DL models, or real-time systems. The practical utility of the ontology in live detection scenarios is yet to be established. **Future work** will involve generating a dataset from the ontology, integrating it with live traffic for real-time DDoS detection, and linking it with DL models to support semantic-based intrusion detection and explainability. Model performance will be evaluated using metrics i.e. **accuracy, precision, recall**, and **F1-score** metrics.

References

[1] Abdussalam Ahmed Alashhab, Mohd Soperi Zahid, Babangida Isyaku, Asma Abbas Elnour, Wamda Nagmeldin, Abdelzahir Abdelmaboud, Talal Ali Ahmed Abdullah, and Umar Danjuma Maiwada. Enhancing ddos attack detection and mitigation in sdn using an ensemble online machine learning model. *IEEE access*, 12:51630–51649, 2024.

[2] Femi Emmanuel Ayo, Joseph Bamidele Awotunde, Lukman Adebayo Ogundele, Olakunle Olugbenga Solanke, Biswajit Brahma, Ranjit Panigrahi, and Akash Kumar Bhoi. Ontology-based layered rule-based network intrusion detection system for cybercrimes detection. *Knowledge and Information Systems*, 66(6):3355–3392, 2024.

[3] Venkata Vivek Gowripeddi, GVK Sasirekha, Jyotsna Bapat, and Debabrata Das. Digital twin and ontology based ddos attack detection in a smart-factory 4.0. In *2023 International Conference on Artificial Intelligence in Information and Communication (ICAIIC)*, pages 286–291. IEEE, 2023.

[4] Mohamed Haddadi, Abdelhamid Khiat, Hadil Bouaoud, and Hadjer Djehiche. Spgdad: Slow http-get denial of service attack detection using ontology. *Information Security Journal: A Global Perspective*, 34(1):79–87, 2025.

d.syeda1@universityofgalway.ie[1], mamoona.asghar@universityofgalway.ie[2]