



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

200
1822 - 2022

Design and Validation of a Reproducible Physical SDN DDoS Dataset for Real-Time Detection Research

Daniel James
2218766

*Man Geni Addysg Uwch yng Nghymru
Where Higher Education Began in Wales*

www.uwtsd.ac.uk

Research Background

- Growth in the use of SDNs in enterprise and cloud networks [1]
- Vulnerabilities in the centralised control plane [2]
- DDoS remains a major threat [3]
- Most research uses either:
 - Simulated environments using Mininet
 - Public legacy datasets (KDD99, CICIDS2017) [1] [3]
- Lack of a realistic SDN-native dataset [4].

Literature Review: Studies on SDN DDoS Detection

Study	Method	Dataset	Environment	Metrics	Limitations
Hassan et al. [5]	DL	InSDN	Simulated	Acc, Prec, Rec, F1	Single dataset
Itagi et al. [6]	DL	Custom dataset	Simulated	Acc	Small dataset
Yu et al. [7]	ML + Entropy	DARPA, CAIDA	Simulated	DR, FAR	Vehicular SDN focus
Belachew et al. [8]	ML	CICIDS2017, Edge-IIoTset	Simulated	Acc, Prec, Rec, F1, Time	SDN-IoT focus
Conti et al. [9]	Statistical	CAIDA, DARPA	Simulated	DR, FAR, Acc, Time	No real deployment

Acc – Accuracy, Prec – Precision, Rec – Recall, F1 – F1-Score, DR – Detection Rate, FAR – False Alarm Rate

Limitations of Existing Network Datasets in SDN Research

Dataset	Environment	Format	Attack Type	Scale / Size	Limitation
InSDN [4]	Simulated SDN	PCAP -> CSV flows	Mixed	~343K flows	Virtual testbed
DARPA [10]	Simulated enterprise	PCAP + logs	Legacy	~9 weeks	Unrealistic simulated traffic
CAIDA [11]	Internet backbone	PCAP	DDoS	~1 hour	Limited attack diversity
CICIDS2017 [12]	Simulated enterprise	PCAP + flows	Modern	~2.8M flows	Controlled environment
Edge-IIoTset [13]	IoT/Edge testbed	PCAP + CSV	IoT attacks	~1M + records	IoT-focused

Research Problem

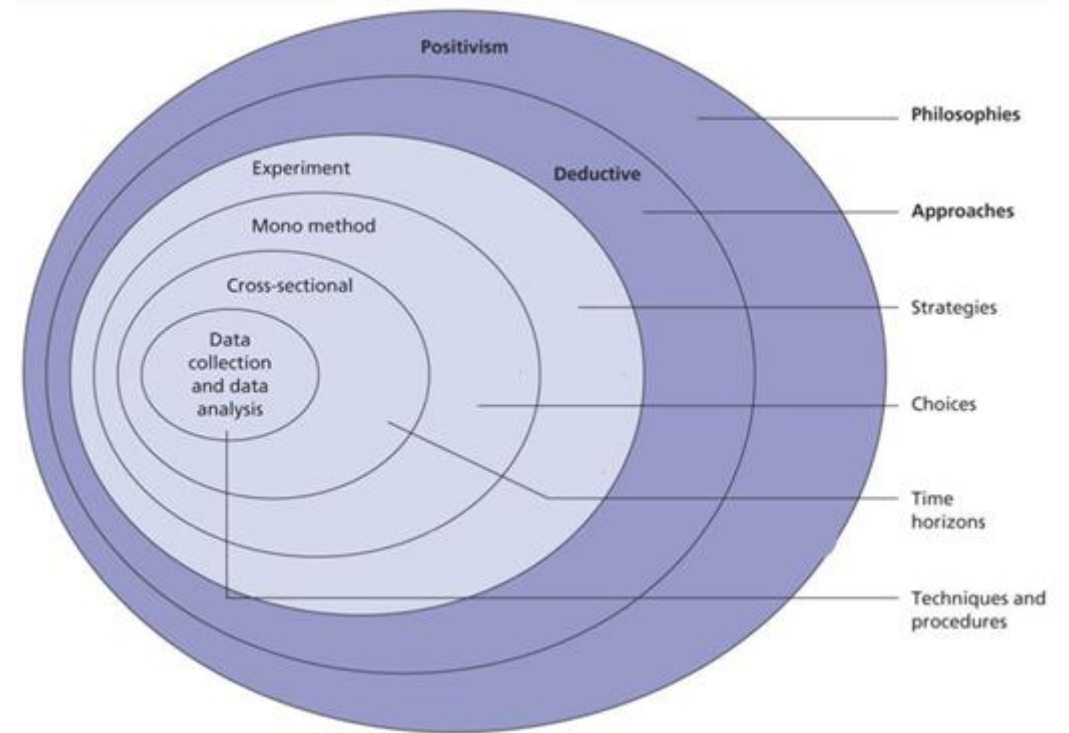
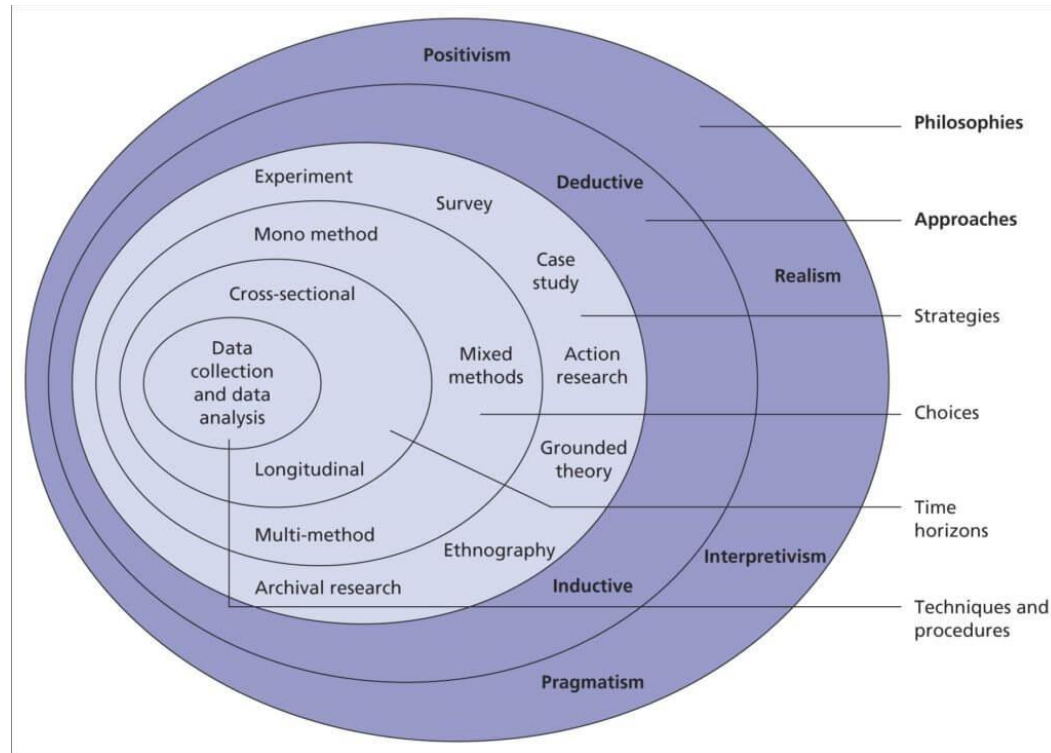
- The lack of properly structured and reproducible physical SDN DDoS datasets reduces the reliability and comparability of existing detection research. Therefore, the creation of a realistic SDN dataset is required.

Aim and Objectives

To design, implement, and validate a physical SDN DDoS dataset, and to evaluate its effectiveness using established DDoS detection techniques.

- Critically analyse existing SDN DDoS datasets to identify methodological gaps.
- Design a methodology for generating a physical SDN DDoS dataset.
- Implement the dataset generation process within a controlled physical SDN lab environment.
- Validate the dataset using established DDoS detection techniques.
- Evaluate detection performance using quantitative metrics.

Research Methodology



Dataset Design

Architecture

- OpenFlow-enabled switches
- SDN Controller
- Legitimate clients
- Attacker machines

Traffic

- Benign Traffic:
 - Web Traffic
 - File Transfers
 - Background Traffic
- Attack Traffic:
 - TCP SYN Flood
 - UDP Flood
 - ICMP Flood
 - Mixed vector attacks
 - Variable attack intensities

Parameters

- Attack duration
- Packet rate
- Number of attacking sources
- Observation window size
- Time synchronisation method

Data Collection and Evaluation

Data Collection

- PCAP capture
- Flow statistics
- Packet in messages
- Controller CPU & memory usage
- Latency measurements

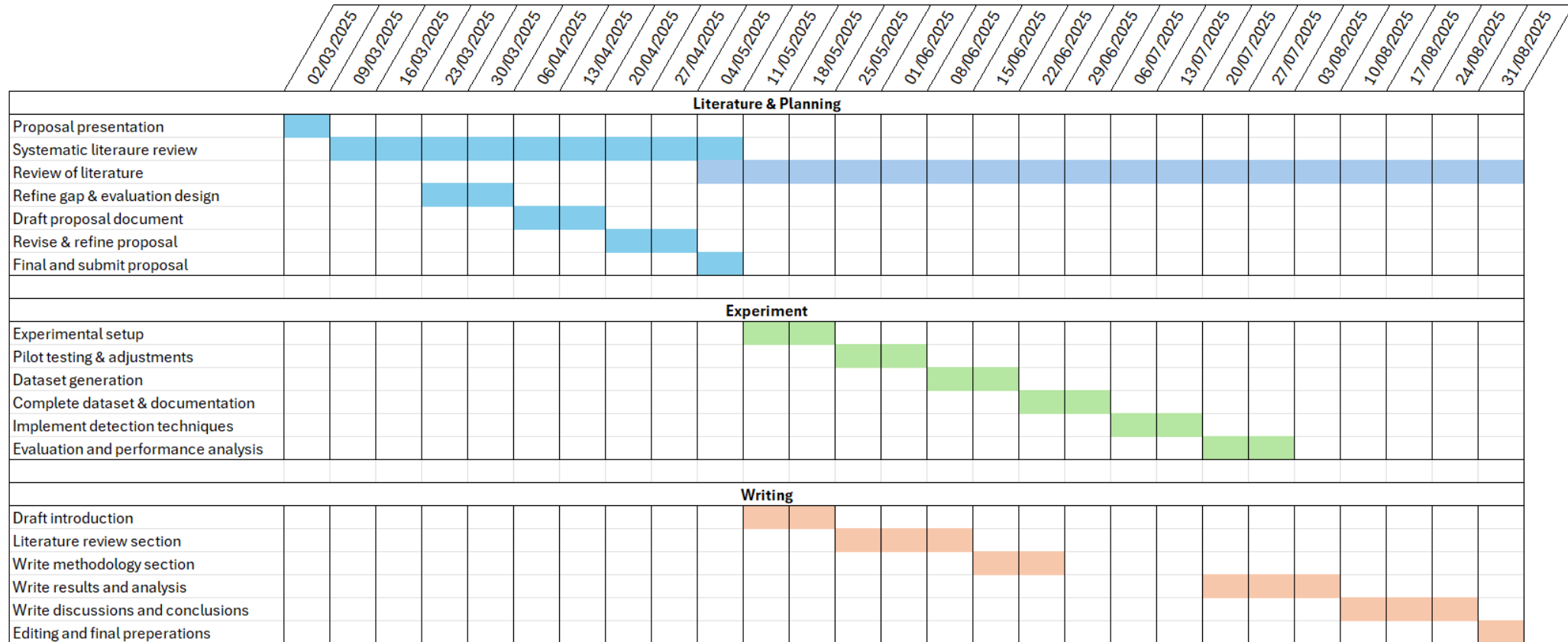
Dataset Structure

- Timestamped flow records
- Attack labels (benign / attack)
- Scenario identifiers
- Structured metadata
- Export formats: CSV + PCAP

Evaluation Strategy

- Entropy-based detection
- ML-based detection
- Accuracy, F1-score, false positive rate
- Detection latency & resource overhead

Project Planning



Impact and Limitations

Impact

- Provides a reproducible physical SDN DDoS dataset
- Supports benchmarking of SDN detection techniques
- Improves methodological rigour in SDN security research
- Potential foundation for future research or publication

Limitations

- Limited hardware scale
- Controlled environment may not reflect real-world traffic complexity
- Time constraints limit attack scenario diversity
- Focus on selected detection techniques

Conclusion

- The lack of a reproducible physical SDN DDoS datasets limit reliable benchmarking.
- This project will design and validate a structured SDN dataset.
- The dataset will be experimentally evaluated using established detection techniques.
- The phased methodology and timeline demonstrate feasibility within the MSc timeframe.

Reference

- [1] D. Kreutz, F. M. V. Ramos, P. Esteves Verissimo, C. Esteve Rothenberg, S. Azodolmolky, and S. Uhlig, "Software-Defined Networking: A Comprehensive Survey," *Proceedings of the IEEE*, vol. 103, no. 1, pp. 14–76, Jan. 2015, doi: <https://doi.org/10.1109/jproc.2014.2371999>.
- [2] S. Scott-Hayward, G. O'Callaghan, and S. Sezer, "Sdn Security: A Survey," *2013 IEEE SDN for Future Networks and Services (SDN4FNS)*, Nov. 2013, doi: <https://doi.org/10.1109/sdn4fns.2013.6702553>.
- [3] S. M. Mousavi and M. St-Hilaire, "Early detection of DDoS attacks against SDN controllers," *2015 International Conference on Computing, Networking and Communications (ICNC)*, Feb. 2015, doi: <https://doi.org/10.1109/iccnc.2015.7069319>.
- [4] M. S. Elsayed, N.-A. Le-Khac, and A. D. Jurcut, "InSDN: A Novel SDN Intrusion Dataset," *IEEE Access*, vol. 8, pp. 165263–165284, 2020, doi: <https://doi.org/10.1109/access.2020.3022633>.
- [5] H. A. Hassan, E. El-Din Hemdan, M. Shokair, F. E. A. El-Samie, and W. El-Shafai, "An Efficient Attack Detection Framework in Software-Defined Networking using Intelligent Techniques," *2023 3rd International Conference on Electronic Engineering (ICEEM)*, pp. 1–6, Oct. 2023, doi: <https://doi.org/10.1109/iceem58740.2023.10319575>.
- [6] V. Itagi, M. Javali, H. Madhukeshwar, P. Shettar, P. Somashekar, and D. G. Narayan, "DDoS Attack Detection in SDN Environment using Bi-directional Recurrent Neural Network," *IEEE Xplore*, Nov. 01, 2021. <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9663667> (accessed Apr. 09, 2023).
- [7] Y. Yu, L. Guo, Y. Liu, J. Zheng, and Y. Zong, "An Efficient SDN-Based DDoS Attack Detection and Rapid Response Platform in Vehicular Networks," *IEEE Access*, vol. 6, pp. 44570–44579, Jul. 2018, doi: <https://doi.org/10.1109/access.2018.2854567>.
- [8] H. M. Belachew, M. Y. Beyene, A. B. Desta, B. T. Alemu, S. S. Musa, and A. J. Muhammed, "Design a Robust DDoS Attack Detection and Mitigation Scheme in SDN-Edge-IoT by Leveraging Machine Learning," *IEEE Access*, pp. 1–1, Jan. 2025, doi: <https://doi.org/10.1109/access.2025.3526692>.
- [9] M. Conti, A. Gangwal, and M. S. Gaur, "A comprehensive and effective mechanism for DDoS detection in SDN," *IEEE Xplore*, Oct. 01, 2017. <https://ieeexplore.ieee.org/document/8115796> (accessed Dec. 04, 2020).
- [10] R. Lippmann, J. W. Haines, D. J. Fried, J. Korba, and K. Das, "The 1999 DARPA off-line intrusion detection evaluation," *Computer Networks*, vol. 34, no. 4, pp. 579–595, Oct. 2000, doi: [https://doi.org/10.1016/s1389-1286\(00\)00139-0](https://doi.org/10.1016/s1389-1286(00)00139-0).
- [11] "The CAIDA 'DDoS Attack 2007' Dataset," *CAIDA*, Feb. 24, 2010. https://www.caida.org/catalog/datasets/ddos-20070804_dataset/
- [12] I. Sharafaldin, A. Habibi Lashkari, and A. A. Ghorbani, "Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization," *Proceedings of the 4th International Conference on Information Systems Security and Privacy*, 2018, doi: <https://doi.org/10.5220/0006639801080116>.
- [13] M. A. Ferrag, O. Friha, D. Hamouda, L. Maglaras, and H. Janicke, "Edge-IIoTset: A New Comprehensive Realistic Cyber Security Dataset of IoT and IIoT Applications for Centralized and Federated Learning," *IEEE Access*, vol. 10, pp. 1–1, 2022, doi: <https://doi.org/10.1109/access.2022.3165809>.