CHAPTER 9

SUMMARY, CONCLUSION AND FUTURE WORK

9.1 Summary and Conclusion

In this thesis, the reader is presented to a new concept towards enhancing IDS solutions for the DDoS attacks identification. In the context of this research, feature engineering is done in detail and necessitates the adoption of multiple ML and DL to improve the detection complexity and outcome. Since feature engineering involves selecting and transforming potential features for data analysis in an effort to significantly enhance ML model proficiency levels, feature engineering is quintessential. However, as the dimension of the modern datasæ is high, traditional methods are unable to find the accurate potential subsets which leads to finding non-optimal feature subset and hence the models which are not so efficient. To address these challenges, this research incorporates complex algorithms and superior methods into the common feature engineering techniques.

The research also employs injected bio-inspiration techniques such as the Improved Dragonfly Optimization Algorithm (IDOA), Panthera Leo Optimization (PLO) for feature selection as the authors aimed at boosting the detection accuracy and minimizing the computational complexity. Furthermore, Approaches such as AEGRN are used in feature extraction to enhance the detection results to various datasets of interest. All these improvements are benchmarked and checked over CICDDoS2019, NSL-KDD+, and the UNSW datasets to nurture reliability, flexibility, and generality.

Filling major existing voids in the existing cybersecurity literature, this work progresses to propose an intelligent IDS that is suitable for detecting single and multiple vector DDoS flooding attacks. Such threats are complicated to identify, and hence the techniques for feature selection, data preparation, and model assessment used in the proposed methodology yield accurate and robust results in identifying these threats. The suggested methodologies are statistically validated for their measurement performance presenting metrics like accuracy, recall, specificity, precision and F1-Score. Some of these procedures are available in forms like ANOVA, p-Test and F-Test that provide rigid disparity checks of the performance of multiple models and conditions. The research follows a structured four-step process to efficiently detect DDoS attacks:

Data Collection: Four datasets are used in the experiments, including CICDDoS2019, UNSW-NB15 and NSLKDD, all of which include various features and labeled instances that are essential for testing the proposed thought. With these datasets, one gets a rich variety attack and benign traffic data in which one can perform the IDS test under different scenarios.

Data Preprocessing: This implies data cleaning which involves features such as duplicates, missing value, outliers and normalization of data for accurate anaysis and modeling. Dealing with missing values make sure that missing data should not affect the results while dealing with outliers, make certain that outliers should not affect the result of the analysis. Normalization scales the information to lessen the effects of having numbers with large magnitude variations. These steps are indispensible while constructing the base that will help in identifying particular and exact kinds of threats, as well as crafting effective defenses against them, helping to steer insightful investigations of the problem.

Feature Engineering and Detection Techniques: The overall IDS has improved in accuracy and resilience due to the feature engineering and detection techniques this paper proposed. This thesis introduces four significant contributions, each proposing different methods for identifying DDoS attacks:

Contribution 1: The Combined Filter for Feature Selection (CFFS) combined with A Decision Tree classifier in identifying individual DDoS flooding assaults gives a new feature selection technique. With precision and recall exceeding 99% with a false positive rate of 6.32%, this method's accuracy was 97.69%. Their performance reduced when extended to multiple flooding attacks; a problem that suggests the need for better techniques for handling such situations.

Contribution 2: Introducing an innovative nature derivative optimization technique known as the Improved Dragonfly Optimization Algorithm (IDOA) while the Decision Tree (DT) classifier is being used concurrently to identify multiple DDoS flooding attacks. This method was proved very efficient with 98.89% accuracy, the precision and recall were above 97%, F-score of 98% and error rate of 4.99%. However, perfecting the model to detect more accurate and efficient solutions is still the requirement.

Contribution 3: This is done with the help of an integrated IDS based on the Panthera Leo Optimization (PLO) associated with a multilayer feedforward network. In a

given IDS, it was possible to keep the Complexity and Variability of the network traffic under control and, at the same time, have a low computed latency and, using the data set CICDDos2019, it was able to achieve for a 96.8% the Prediction accuracy.

Contribution 4: Introducing an IDS that applies the AEGRN model for detecting DDoS attacks for multiple datasets. Above 98% generalization, the IDS provided a better detection accuracy across various datasets within an average time of 17.4 s per epoch though the Op-LSTM, GRU and LSTM models were comparatively faster. Self-attention maps integrated with BiGRU and feedforward proved useful for classification less complexity and time.

Performance Evaluation: The last stage is to analyze the efficacy of the suggested approaches to the databases under consideration by examining the current performance metrics like F1-Score, Accuracy, Recall, Specificity, and Precision. By collecting the appropriate formulations for false positives and false negatives along with real positives and the converse, these metrics gives an extensive and accurate evaluation of the IDS's results. When methods are applied to real-world situations, statistical validation helps to lower the uncertainty of the results by offering a reliable benchmark of the corresponding performance parameters. Such parameters as ANOVA, p-Test, F-Test are used to endorse seen improvements in the performance between models stating that these improvements are not random. This makes sure that IDS actually captures the DDoS attacks while avoiding unnecessary alarms and misses, making the tool extremely useful in real world.

Based on the experiments, results and validation, the Phase IV comprises the most sophisticated and efficient intelligent detection system created by this study. By implementing A Bernardino et al. architecture known as the Attention-Enabled Gated Recurrent Networks (AEGRN) and the Deep Feed Forward Networks Phase IV outperforms earlier stages in terms of metrics and datasets, including UNSW, NSL-KDD+(Train), NSL-KDD+(Test), and CICDDoS2019. This section's findings further demonstrate that the suggested model outperforms LSTM, GRU, and optimized-GRU with respect to accuracy. Specifically, it is acknowledged that the proposed model's accuracy and precision are maximal; the comparison with other models demonstrates that the differences are significant.

In addition, Phase IV’s efficiency is observable in the model building times and the proposed model indicates the shortest MBT across all datasets. This cuts the computational

overhead considerably which is necessary for making the solution usable, making DDoS assaults may be quickly detected and countered. Given the very low RMSE between the training and testing datasets, the validation curves further bolster this claim, hence increasing the reliability of the model in different situations.

In conclusion, compared with the four contributions, the intelligent detection system proposed in Phase IV fully uses the bionic algorithm AEGRN and Deep Feed Forward Networks, which is the most advanced and efficient identification method. Not only does it offer the best performance in comparison to the other algorithms, but it also realizes the fastest computation, which gives it the potential of becoming an important tool in strengthening the protection against new complex types of DDoS attacks. In reference to these theories, this thesis presents a comprehensive plan to improve IDS against DDoS through feature engineering and implementation of ML and DL. The level of structure, requirement for evaluation, and timely provision of contributions make the proposed methodology credible for enhancing cybersecurity efficiently.

9.2 Future Scope

Based on the progress of the research made in this thesis, future studies should focus on two significant aspects to contribute to the improved versatility of the given IDS in real environments. First of all, the effectiveness of the developed model has to be confirmed on real-time datasets. Benchmark datasets provide insights, experiments on current, real datasets are needed to mimic real-world problems and capture facets missed in a controlled environment. By doing this validation, we will get a better estimative of the system's flexibility and effectiveness in facing new cyber threats.

Secondly, it is vital to determine not only the capability of the model in identifying and mitigating AI enhanced and Deep DDoS threats, attack types. These attacks will employ artificial intelligence to change its attack patterns in response to the target making it even more complex and difficult to identify. Testing the system is possible using both AI-Enhanced DDoS prototype attacks and real AI-Enhanced DDoS attacks will help to determine its performance in real-life scenarios and estimate the system's ability to cope with contemporary threats. It will ensure the system is robust and reliable enough to counter modern and ever-changing cyber threat practices.

9.3 Real-World Applicability: Case Studies and Practical Insights

In addition to experimental validation, this research considers the practical deployment conditions under which intrusion detection systems must function. These environments often involve constraints such as limited computational resources, high data throughput, and constantly evolving network traffic. The models proposed across the four phases of this thesis have been designed with these real-world considerations in mind. To further demonstrate their applicability, the following case studies present how similar strategies have been successfully implemented in commercial and cloud-based security infrastructures thereby reinforcing the practical significance of the proposed methodologies.

Case Study 1: Amazon Web Services (AWS) provides a managed DDoS protection service known as AWS Shield, which uses machine learning techniques to detect and mitigate threats in real time. (Amazon Web Services. 2023). It operates by continuously monitoring network traffic, applying rule-based filtering, and leveraging anomaly detection to identify suspicious patterns. While the exact algorithms are proprietary, the design reflects an industry-wide shift toward using lightweight machine learning models for initial threat screening, followed by more advanced mechanisms for deeper analysis.

This approach closely parallels the method proposed in Phase I of this thesis, where an ensemble-based combined filter is used for feature selection and paired with a Decision Tree classifier to achieve high detection accuracy with low computational overhead. Like AWS Shield, the Phase I framework emphasizes fast, interpretable, and resource-efficient detection making it well-suited for real-time environments

Case Study 2: The CICFlowMeter-V3 tool, developed by the Canadian Institute for Cybersecurity (Lashkari, A.H., et al. 2017)., is widely used for generating flow-based network traffic features from raw packet captures. It is a key tool behind datasets such as CICDDoS2019, which has been adopted across industry and academia to simulate real-world DDoS scenarios.

This thesis uses CICDDoS2019 extensively for model training and validation. The dataset's design, based on real attack tools and multi-vector scenarios ensures that the models developed are tested under near-deployment conditions. In particular, the proposed AEGRN and PLO-MLFFN models (Phases III and IV) are validated using this dataset, aligning closely with the kind of traffic patterns encountered in production networks. The

key relevance confirms that the models are trained and tested on datasets created to mimic real-world DDoS attack behavior enhancing their transferability to actual network infrastructures.

Case Study 3: Google Cloud Armor offers a cloud-based protection service aimed at defending applications against large-scale and sophisticated threats, including application-layer (Layer 7) DDoS attacks (Google Cloud. 2023). Its Adaptive Protection feature employs unsupervised machine learning techniques to dynamically learn baseline traffic patterns and detect deviations that may indicate malicious activity. This system continuously adapts to new behaviors by analyzing traffic trends and triggering mitigation when abnormal patterns are observed.

The integration of this mechanism within Google's global load balancing infrastructure allows for automatic anomaly detection and response, without relying on pre-labeled training data. This capability is particularly effective in identifying stealthy or low-rate DDoS attacks that often evade traditional detection systems. The approach shares strong alignment with the methodology proposed in Phase IV of this thesis, where an Attention-Enabled Gated Recurrent Network (AEGRN) is used to enhance detection accuracy by capturing temporal dependencies and focusing on critical features within complex traffic sequences. Google Cloud Armor illustrates the practical utility of adaptive, attention-based learning models, similar to the AEGRN architecture proposed in this research. It reinforces the feasibility and effectiveness of deploying intelligent IDS frameworks that can generalize across diverse datasets and adjust to evolving attack vectors.