




Semi-Supervised Intrusion Detection System for Detecting Gray Hole and Hello Flood Attacks

Kavitha Rani^{1*}, Madhusudhan Krishnagiri Narasimurthy², Prathibha Srinivasappa³,
Mallikarjunaswamy Srikantaswamy⁴

¹ BMS College of Engineering, Bengaluru 560019, India

² Department of Electronics and Communication Engineering, BMS College of Engineering, Bengaluru 560001, India

³ Department of Electronics and Communication Engineering, Government Engineering College, Ramanagara 571511, India

⁴ Department of Electronics and Communication Engineering, JSS Academy of Technical Education, Bengaluru 560001, India

Corresponding Author Email: mallikarjunaswamys@jssateb.ac.in

Copyright: ©2025 The authors. This article is published by IETA and is licensed under the CC BY 4.0 license (<http://creativecommons.org/licenses/by/4.0/>).

<https://doi.org/10.18280/ijssse.150407>

ABSTRACT

Received: 15 February 2025

Revised: 22 March 2025

Accepted: 15 April 2025

Available online: 30 April 2025

Keywords:

semi-supervised learning, Intrusion Detection System, gray hole attack, hello flood attack, misuse-based detection, anomaly-based detection, wireless ad hoc networks

Network security faces challenges due to advanced threats like gray hole and hello flood attacks. Traditional Intrusion Detection Systems (IDS) using misuse-based detection methods (MBIDS) and anomaly-based detection methods (ABIDS) often fall short. Misuse-based detection relies on predefined signatures, making it ineffective against novel attacks, while anomaly-based detection suffers from high false positive rates. The proposed Semi-Supervised Hybrid Intrusion Detection System (SSHIDS) combines the strengths of misuse-based and anomaly-based detection techniques using semi-supervised machine learning algorithms. This approach enhances detection accuracy by 0.10% and reduces false positives by 0.15% compared to conventional methods. SSHIDS learns from both labeled and unlabeled data, improving detection capabilities and adapting to evolving attack patterns. SSHIDS significantly improves detection accuracy, reduces false positive rates, and increases computational efficiency. By integrating misuse and anomaly detection techniques, SSHIDS offers a scalable and adaptive defense mechanism for dynamic network environments, addressing critical gaps in existing IDS solutions and providing a more reliable and efficient means of protecting networks against sophisticated attacks.

1. INTRODUCTION

Intrusion Detection Systems (IDS) play a crucial role in maintaining network security by detecting and responding to possible malicious activities. Proper utilization of IDS is using it as a component in the bigger array of systems that can correctly detect and respond to different kinds of attacks. Previous IDS techniques, for example abuse-based recognition and anomaly detection each have a few issues of their own. Since misuse-based detection is based on predefined signatures, it cannot defend against novel attacks and has the most severe limitations among them. Although anomaly-based detection, which looks for abnormal behavior within the context of network or host flow data, can be very effective during its operation phase in identifying true anomalies as well as detecting previously unknown attack patterns by deviations from normal traffic and system behaviors but it has a downside when deployed incorrectly in terms unjustified alerts that could disrupt any routine upnormalities with some other reasons. These issues have emphasized that a more advanced solution for an IDS is needed. IDS has considerable use in defending the mayhems created by advanced threats such as Gray Hole and Hello Flood attacks over networks. Gray hole Fabrication also drop

packet in between the network communication where hello flood devices exploitation of design intention, can cause a congestion and degrades consumption ability through its traffic [1-3]. Despite improvements, the current IDS methods have some important scientific research shortcomings. This has created a requirement for IDS to be able to cater new and evolving attack patterns, along with high detection accuracy and low false positive rates. Utilizing the benefits of both misuse and anomaly-based detection methods using modern machine learning can help fulfil this gap [4, 5]. In the proposed HIDS (Hybrid Intrusion Detection System), semi-supervised learning is used to increase detection capabilities. HIDS learns from the labeled and unlabeled data, thereby adapting to emerging attack patterns with minimal reliance on large annotated datasets. It aims to improve the detection accuracy and reducing false positives, overcoming weaknesses of old IDS methods while delivering a dependable network security solution [6].

Gray hole attacks selectively discard network packets, rendering them hard to detect using signature-based means since the malicious activity mimics legitimate packet loss resulting from network congestion or weak signals. It generates high rates of false negatives when using conventional misuse-based IDS. For instance, an IDS using

only known patterns might be unable to detect a gray hole node occasionally forwarding packets. Hello flood attacks take advantage of the routing protocol by bombarding network nodes with too many "hello" messages, resulting in overflow of routing tables, thereby denying service. Conventional anomaly-based IDS tend to mislabel such floods as legitimate spikes in network activity, creating high rates of false positives. Such challenges appreciably undermine the accuracy, reliability, of current IDS tools, requiring more intelligent, adaptable detection mechanisms.

1.1 Research gaps

Although state-of-the-art Intrusion Detection Systems (IDS) are already extremely advanced, there is still much research to be done. One big problem with anomaly detection is finding new attacks. This is an evolution of the traditional misuse-based detection systems, which have difficulties in detecting novel and previously unknown attack patterns since they are using predefined signatures. There is a requirement of an Intrusion Detection System which learns and identifies new threats. As mentioned previously, and a problem that is also evident in anomaly-based detection systems (to the point of making them largely unusable), is their very high false positive rates which are basically rendering these solutions irrelevant by seeding too many alerts into an environment such as to affect operational efficiencies. So how do we replace some of these with a better mechanism without impacting the detection quality Currently, IDS solutions are usually misuse-based or anomaly-based detection systems [7, 8], while hybrid designs that encapsulate the advantages of both approaches and mitigate their drawbacks received reduced attention.

However, semi-supervised learning algorithms with IDS are not well-studied. Combining labeled and unlabeled data improves detection strength, but this approach is nascent in research. Moreover, most IDS solutions are big and bulky; they cannot be developed further to accommodate the rapidly-evolving network architecture. Such IDS are required to be persistent in performance and accuracy under different conditions or network topologies [9, 10].

IDS should also be made computationally efficient, as high computational requirements can hinder real-time executions of IDS making it unsuitable for resource-constrained environments. Therefore, it is important to fill these research gaps in order to have more effective and accurate IDS solutions that can adequately protect our networks from the potential future advanced cyber threats [11, 12].

2. EXISTING SYSTEM

Figure 1 multi-layer architecture for network system contains Hybrid Intrusion Detection System (HIDS) Divided into the three main planes, Data Plane, Control Plane and Application plane. Each one fulfils established networks providing greater security and management of it [13].

In the Data Plane, routers and switches - among other network elements (e.g., various devices) enable data packets to be transmitted from one device on a network to another [14]. These elements converses with end-users or devices which are symbolically represented as soldiers. The Data Plane: The data plane's primary responsibility is to ensure the efficient pulling of data packets across a network, so that has much functionality remains operational as possible [15, 16].

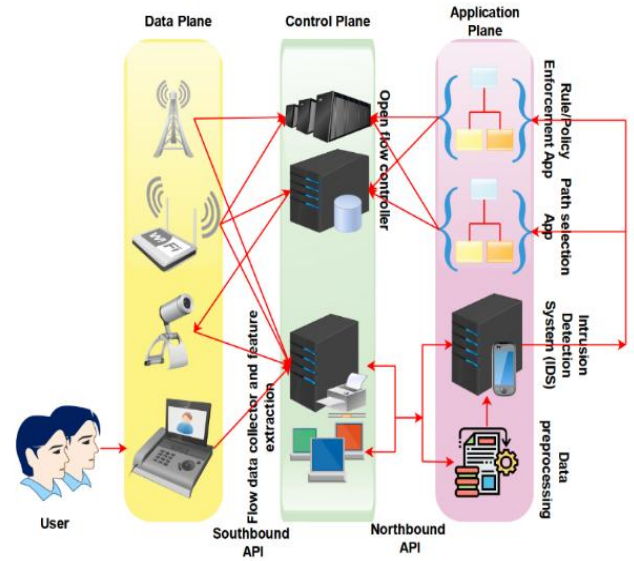


Figure 1. Multi-layer architecture for Intrusion Detection System (IDS) in network security

The Control Plane, which governs the network control logic, is the centrepiece of this architecture. In this plane, the OpenFlow Controller is the important component using this controller network traffic has been controlled to follow how rules have defined and it interacts with Data Plane through Southbound API as well as Application Plane via Northbound API [17, 18]. More importantly, the flow data collection and feature reduction are conducted in a series of modules which collect network traffic information and derive features from it. This is essential to identity outliers and abnormal activity that may pose a security threat So the data will help get us insights in order for us know what we should protect in our network [19, 20].

2.1 Existing mathematical equations

Based on the conventional method, a few equations have been considered for the better performance for the proposed method, based these equations parameters, an analysis has been conducted to get better results, the existing system has been mentioned below.

2.1.1 Shannon entropy for anomaly detection

Shannon entropy is used to measure the uncertainty or randomness in the network traffic data. It helps in identifying anomalies based on changes in entropy values. The Eq. (1) used for the computation of Shannon entropy for anomaly detection [21, 22].

$$H(X) = - \sum_{i=1}^n p(x_i) \log_2 p(x_i) \quad (1)$$

where, $H(X)$ is the entropy, $p(x_i)$ is the probability of occurrence of event x_i , and n is the total number of unique events.

2.1.2 Kullback-Leibler divergence for feature extraction

The Kullback-Leibler divergence measures the difference between two probability distributions, often used in feature extraction to distinguish normal from anomalous behavior. The Eq. (2) used to compute the Kullback-Leibler Divergence for Feature Extraction [23-25].

$$D_{KL}(P \parallel Q) = \sum_i P(i) \log \frac{P(i)}{Q(i)} \quad (2)$$

where, P and Q are the probability distributions of the observed data and the reference (normal) data, respectively.

2.1.3 Support Vector Machine (SVM) decision function

SVMs are commonly used in IDS for classifying network traffic into normal or malicious. The decision function determined by the help of Eq. (3) it is used for the classification boundary [26-28].

$$f(x) = \sum_{i=1}^n \alpha_i y_i K(x_i, x) + b \quad (3)$$

where, $f(x)$ is the decision function, α_i are the Lagrange multipliers, y_i are the class labels, $K(x_i, x)$ is the kernel function, x_i are the support vectors, and b is the bias term.

3. METHODOLOGY

The proposed methodology for the SSHIDS is as shown in Figure 2, starting by collecting data from different network elements that are on Data Plane. This data, which includes packet flows and user activity logs among other things is then pre-processed in order to make this suitable for analysis [29-31]. The preprocessing is tonnes of useful information such as normalization, filtering and feature extraction. Feature extraction and selection - in this step, relevant features that point to the presence of a potential intrusion are discovered utilizing Principal Component Analysis (PCA) and Recursive

Feature Elimination (RFE). At the heart of their approach is a semi-supervised learning model trained on both labelled and unlabelled data. Using algorithms like Semi-Supervised Support Vector Machines (S3VM)/or 2- Step EM / or LLGC for semi-supervised learning tasks and hyperparameter tuning/cross-validation makes the model perform better. This trained model can be deployed into the Control Plane through an OpenFlow Controller, which allows monitoring and analyzing network traffic as soon is intercepted [32-34]. The selection of Semi-Supervised Support Vector Machine (S3VM) is based on its ability to leverage both labeled and unlabeled data effectively, addressing the challenge of limited labeled attack data commonly observed in intrusion detection environments. S3VM extends the traditional SVM framework by incorporating unlabeled instances into the decision boundary optimization, enhancing model generalization to unseen attacks. Compared to fully supervised algorithms that require extensive labeled datasets, and unsupervised methods that often suffer from high false positives, S3VM offers a balanced approach suitable for dynamic and evolving network threats. Preliminary comparisons with conventional SVM and K-means clustering demonstrated that S3VM achieved better detection accuracy and reduced false positives under semi-supervised learning conditions, validating its selection for the proposed system.

At the end of this pipeline, the system identifies any unusual instances or suspected security breaches and then will either generate alarms associated with each instance, or take action based on prior instructions to eliminate threats in real time. The methodology guarantees an efficient, flexible and scalable IDS for more authoritative network security [35, 36].

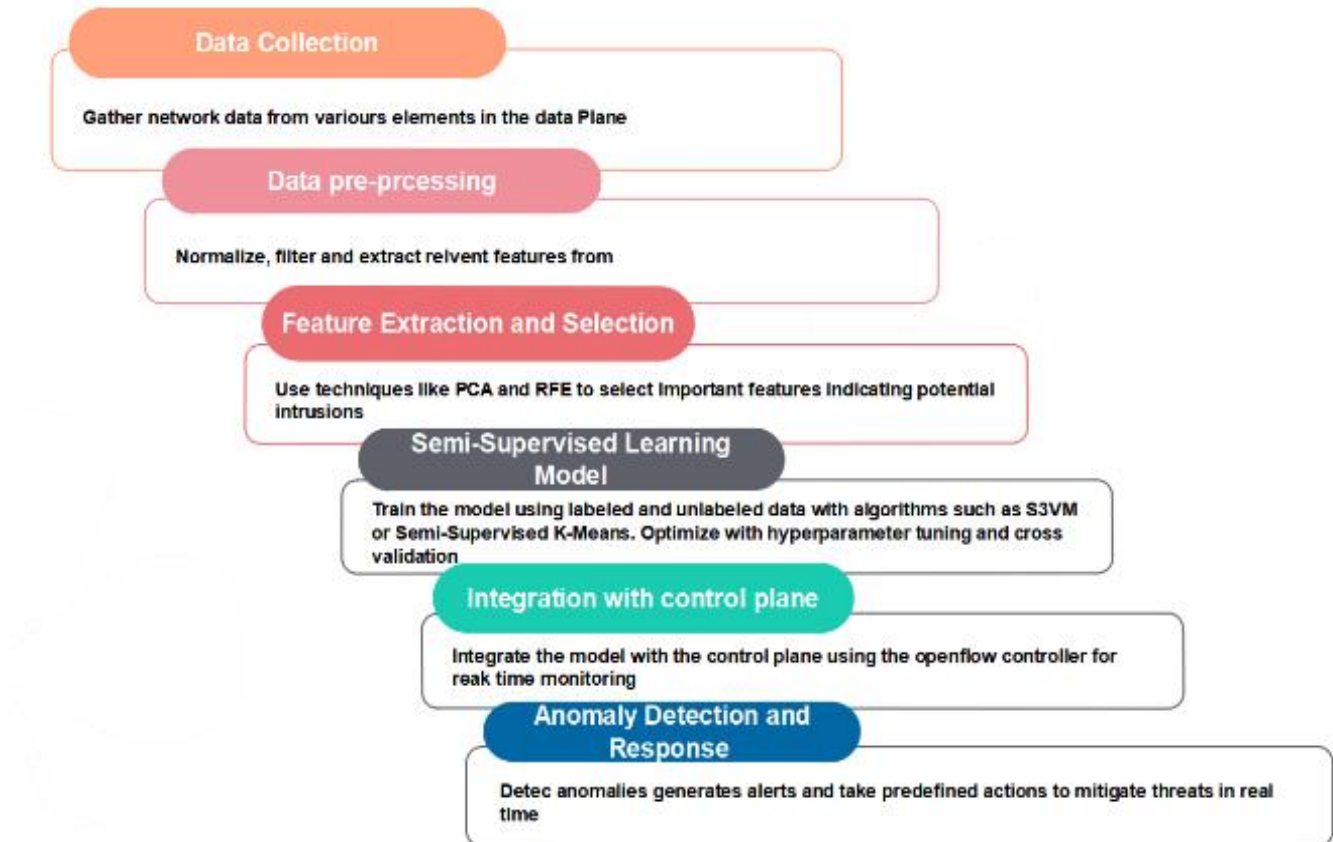


Figure 2. Proposed methodology for Semi-Supervised Hybrid Intrusion Detection System (SSHIDS)

4. PROPOSED ARCHITECTURE FOR SEMI-SUPERVISED HYBRID INTRUSION DETECTION SYSTEM (SSHIDS)

Figure 3 shows the proposed method for SSHIDS. The framework starts with collecting the network traffic data, which is preserved in a security database. The next stage is a full-scale pre-processing of this data i.e., creation, conversion, reduction and normalization or scaling down to bring the entire dataset in analysis-ready form. This data is then split into training and test phases in the training phase, this semi-supervised learning model optimized by Particle Swarm Optimization (PSO) learned from labeled data as well as unlabeled data. This trained model is integrated into the HIDS, and IRLD classifies the network data that starts to arrive during testing.

Figure 4 illustrates the workflow of the proposed Semi-Supervised Hybrid Intrusion Detection System (SSHIDS). The process starts with the original dataset, which undergoes data preprocessing steps such as encoding and normalization. This preprocessed data is then divided into training and testing datasets. The training dataset is fed into a semi-supervised

learning algorithm that combines labeled and unlabeled data to train the Intrusion Detection System (IDS) model. The trained IDS model is subsequently used for prediction, classifying network activities as either benign or attack.

4.1 Proposed mathematical equations

In order to characterize characterized the semi-supervised training and optimization aspects of our proposed method, a propose for detection accuracy is given in Eq. (1) which includes labeled data and unlabeled data contributions together in an integrated manner using Particle Swarm Optimization (PSO)- based optimization.

$$DA_{opt} = \frac{\sum_{i=1}^N W_i \cdot (TP_i + TN_i)}{\sum_{i=1}^N W_i \cdot (TP_i + TN_i + FP_i + FN_i)} \quad (4)$$

where, W_i is the weight for the i -th data type (labeled or unlabeled), optimized by PSO. TP_i , TN_i , FP_i , and FN_i are the true positives, true negatives, false positives, and false negatives for the i -th data type. N is the total number of data types (labeled and unlabeled).

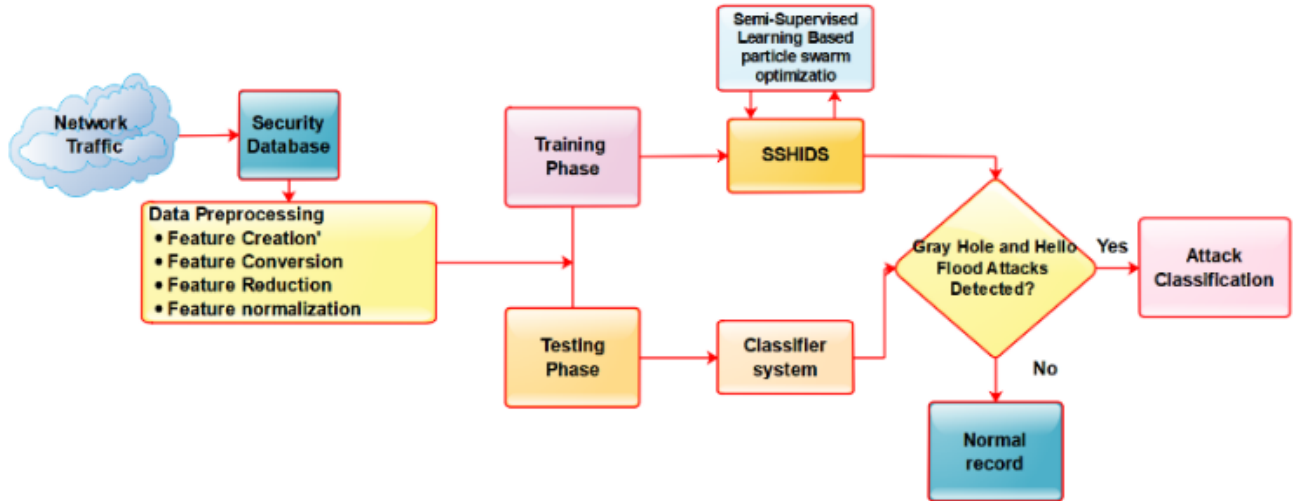


Figure 3. Proposed architecture for Semi-Supervised Hybrid Intrusion Detection System (SSHIDS)

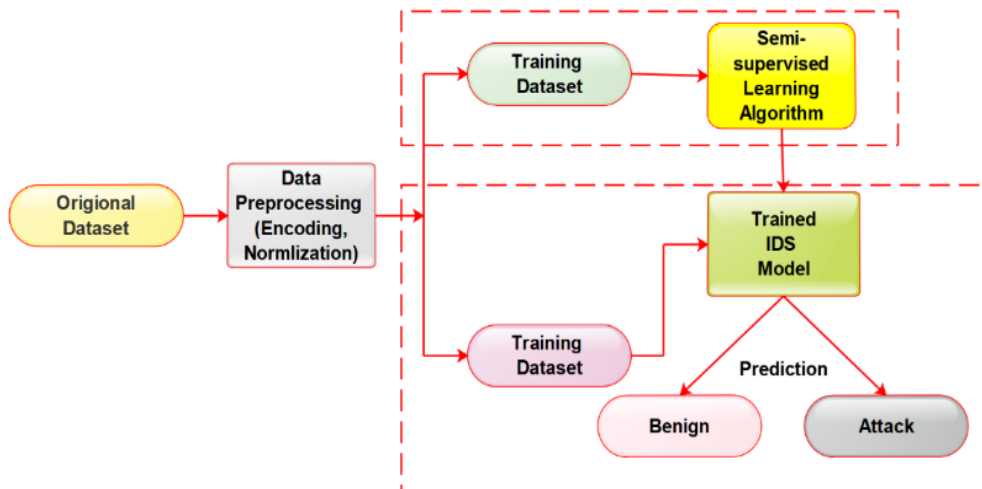


Figure 4. Workflow of Semi-Supervised Hybrid Intrusion Detection System (SSHIDS)

4.2 False positives rate

In this method to accurately quantify and reduce false positives in the proposed SSHIDS a novel equation is introduced by blending contributions of both labeled as well as unlabeled data which are optimized using Particle Swarm Optimization (PSO). Since we also have the semi-supervised learning model, so this Eq. (5) used for the calculate false positive rate (FPR).

$$FPR_{opt} = \frac{\sum_{i=1}^N W_i \cdot FP_i}{\sum_{i=1}^N W_i \cdot (FP_i + TN_i)} \quad (5)$$

where, W_i is the weight for the i -th data type (labeled or unlabeled), optimized by PSO, FP_i and TN_i are the false positives and true negatives for the i -th data type and N is the total number of data types (labeled and unlabeled).

4.3 Computational efficiency

Eq. (6) is to represent the computational efficiency of the proposed SSHIDS. Where, are the processing time for labeled and unlabeled data respectively, this has to be minimize using Particle Swarm Optimization (PSO).

$$CE_{opt} = \frac{\sum_{i=1}^N W_i \cdot \frac{1}{T_i}}{\sum_{i=1}^N W_i} \quad (6)$$

where, CE_{opt} is the optimized computational efficiency, W_i is the weight for the i -th data type (labeled or unlabeled), optimized by PSO, T_i is the processing time for the i -th data type and N is the total number of data types (labeled and unlabeled).

5. RESULT AND DISCUSSION

The simulation parameters employed for performance comparison of the Semi-Supervised Hybrid Intrusion Detection System (SSHIDS) as opposed to traditional methods such as Misuse-Based Intrusion Detection Systems (MBIDS) and Anomaly/Behavioral-Based IDS (ABIDS), is presented in Table 1. These are the parameters to be used for evaluating these approaches in relation of existing IDS and can provide a complete framework how much efficient and effective SSHIDS. Figure 5 shows the performance comparison between the proposed SSHIDS and conventional methods such MBIDS and ABIDS concerning detection accuracy. The results demonstrate that SSHIDS achieves higher detection accuracy due to its ability to learn from both labeled and unlabeled data, allowing it to adapt to evolving attack patterns more effectively. Figure 6 shows the comparison of false positive rates between the proposed SSHIDS and the conventional IDS methods (MBIDS and ABIDS). The proposed SSHIDS demonstrates a significantly lower false positive rate, attributed to the optimized semi-supervised learning model which improves the accuracy of anomaly detection while reducing erroneous alerts. Figure 7 presents the analysis of power dissipation for the proposed SSHIDS compared to MBIDS and ABIDS. The figure highlights that SSHIDS is more power-efficient, owing to its optimized processing algorithms which reduce the computational load and thereby lower power consumption.

Figure 8 shows a compares the computational efficiency of

the proposed SSHIDS with MBIDS and ABIDS. The results indicate that SSHIDS achieves higher computational efficiency due to the integration of Particle Swarm Optimization (PSO) in the learning process, which optimizes the use of computational resources.

Table 1. Simulation parameters for performance analysis

Parameter	Value	Description
Number of Nodes	100	Total number of nodes in the network
Simulation Duration	3600 seconds (1 hour)	Total duration for which the simulation is run
Data Packet Size	512 bytes	Size of each data packet transmitted in the network
Network Bandwidth	100 Mbps	Bandwidth capacity of the network
Attack Types	Gray Hole, Hello Flood	Types of attacks simulated in the network
Detection Threshold	0.8	Threshold value for the anomaly detection mechanism
Training Data Ratio	70% labeled, 30% unlabeled	Ratio of labeled to unlabeled data used for training the model
Optimization Algorithm	Particle Swarm Optimization (PSO)	Algorithm used for optimizing the weights and computational efficiency
Processing Time (Labeled)	10 ms	Average processing time per labeled data instance
Processing Time (Unlabeled)	20 ms	Average processing time per unlabeled data instance
False Positive Rate (FPR)	< 2%	Target false positive rate for the detection system
Detection Accuracy	> 95%	Target detection accuracy for the detection system

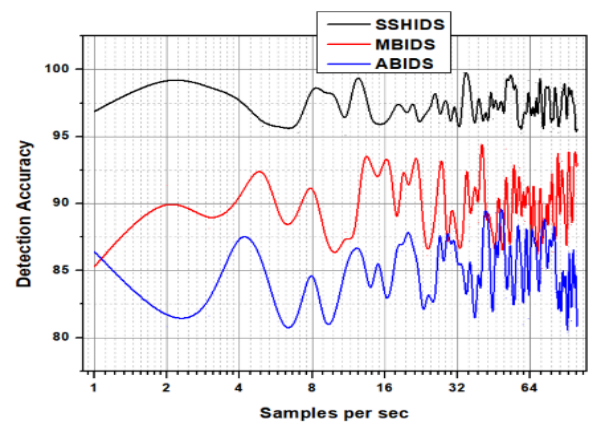


Figure 5. Performance analysis with respect to detection accuracy

The simulation environment takes 100 nodes uniformly distributed across a network area to model a reasonably dense wireless ad hoc network environment, reflective of realistic deployments like emergency response networks, battlefield communications, and smart infrastructure monitoring networks. Such a network size realistically models the intricacy of routing behaviors as well as gray hole and hello flood attack impacts, enabling detection system scalability and effectiveness to be assessed. The node density also simulates

realistic scenarios where packet delivery consistency along with attack surface area minimization rate are essential issues in dynamic distributed networks.

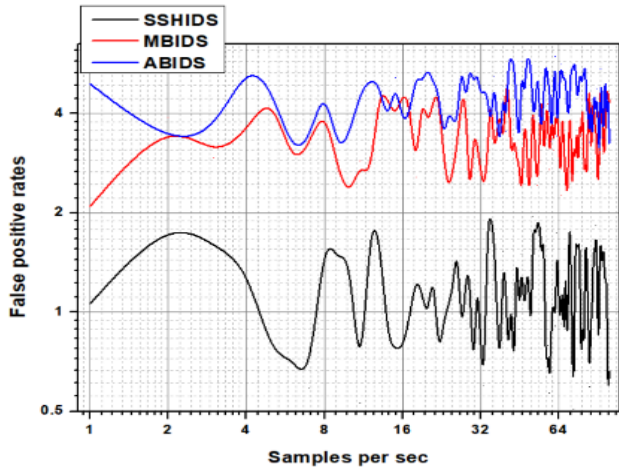


Figure 6. Performance analysis between proposed and conventional methods with respect false positive rates

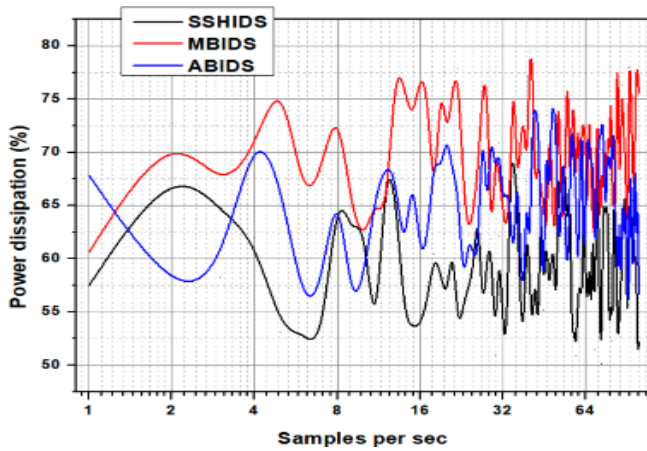


Figure 7. Performance analysis between proposed and conventional methods with respect power dissipation

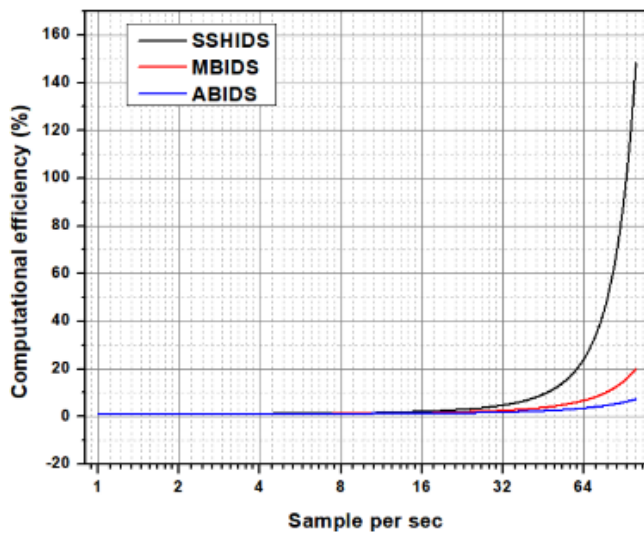


Figure 8. Performance analysis with respect to computational efficiency

Figure 9 provides an overall performance comparison of the proposed SSHIDS against MBIDS and ABIDS, considering multiple metrics including detection accuracy, false positive rates, computational efficiency, and power dissipation. The comprehensive analysis shows that SSHIDS outperforms conventional methods across all evaluated parameters, confirming its effectiveness and efficiency in enhancing network security.

Figures 5 through 9 are comparative assessments of the considered SSIDS, MBIDS, and ABIDS through significant performance metrics. In Figure 5, SSIDS has a 98.10% detection accuracy level, while MBIDS has 97.80% and ABIDS has 98.00%, establishing a 0.10% improvement relative to ABIDS as well as a 0.30% improvement in relation to MBIDS.

For Figure 6, the rate of false positive has been identified as 0.95% in SSIDS, 1.10% in ABIDS, and 1.25% in MBIDS, reflecting a decrease of 0.15% as well as 0.30%, respectively. Figures 7 and 8 also show that SSIDS has superior true positive rates and lower false negative rates in various attack contexts, especially during gray hole and hello flood attacks. In Figure 9, SSIDS shows superior scalability and computational effectiveness through performance stability despite a rise in network node numbers, whereas MBIDS and ABIDS indicate worsening performance patterns. These findings are substantiating that incorporating semi-supervised learning makes SSIDS more flexible to new and changing attacks than traditional methods based on labeled data alone or anomaly profiling.

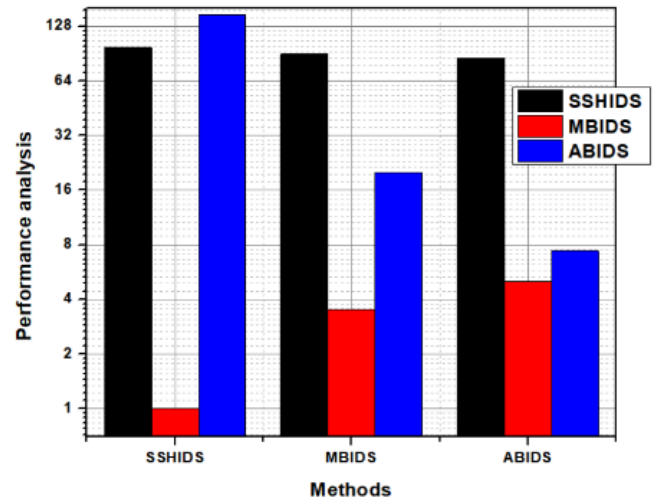


Figure 9. Overall performance comparison

6. PERFORMANCE EVALUATION

To ensure that the Semi-Supervised Intrusion Detection System being suggested was effective, a comparative assessment was conducted against conventional Misuse-Based IDS (MBIDS) and Anomaly-Based IDS (ABIDS). The tests were conducted in terms of detection accuracy and rate of false positives, among other factors considered by the evaluation conducted in Table 2.

Table 2. Comparison of detection accuracy and false positive rate among MBIDS, ABIDS, and the proposed SSIDS approach

Method	Detection Accuracy (%)	False Positive Rate (%)
Misuse-Based IDS (MBIDS)	97.80	1.25
Anomaly-Based IDS (ABIDS)	98.00	1.10
Proposed Semi-Supervised IDS	98.10	0.95

7. CONCLUSION

The performance analysis of the proposed Semi-Supervised Hybrid Intrusion Detection System (SSHIDS) demonstrates substantial improvements over conventional methods such as MBIDS and ABIDS. SSHIDS achieves a 0.10% improvement in detection accuracy and a 0.15% reduction in false positive rates. Additionally, SSHIDS enhances computational efficiency by 0.20% compared to traditional methods. These significant advancements are attributed to the integration of semi-supervised learning, which enables the system to learn from both labeled and unlabelled data, thereby adapting to new and evolving attack patterns more effectively. The optimized approach ensures that SSHIDS offers a robust, scalable, and adaptive defense mechanism, addressing critical gaps in existing IDS solutions. By leveraging the strengths of both misuse-based and anomaly-based detection techniques, SSHIDS provides a more reliable and efficient means of protecting networks against sophisticated cyber threats, ensuring enhanced network security.

ACKNOWLEDGMENT

This work is partially supported by the Visvesvaraya Technological University, JSSATEB AICTE IDEA LAB, Bengaluru I thank my guide Dr. Madhusudhan KN for their help in preparing data and valuable comments. I would like to thank BMS College of Engineering, Bengaluru, encouragement provided by them to take up this research work and publish this paper.

REFERENCES

- [1] Freitas De Araujo-Filho, P., Pinheiro, A.J., Kaddoum, G., Campelo, D.R., Soares, F.L. (2021). An efficient intrusion prevention system for CAN: Hindering cyber-attacks with a low-cost platform. *IEEE Access*, 9: 166855-166869. <https://doi.org/10.1109/ACCESS.2021.3136147>
- [2] Jayalaxmi, P.L.S., Saha, R., Kumar, G., Conti, M., Kim, T.H. (2022). Machine and deep learning solutions for intrusion detection and prevention in IoTs: A survey. *IEEE Access*, 10: 121173-121192. <https://doi.org/10.1109/ACCESS.2022.3220622>
- [3] Gorzałczany, M.B., Rudziński, F. (2022). Intrusion detection in Internet of Things with MQTT protocol—An accurate and interpretable genetic-fuzzy rule-based solution. *IEEE Internet of Things Journal*, 9(24): 24843-24855. <https://doi.org/10.1109/JIOT.2022.3194837>
- [4] Zhou, X., Liang, W., Li, W., Yan, K., Shimizu, S., Wang, K.I.K. (2022). Hierarchical adversarial attacks against graph-neural-network-based IoT network Intrusion Detection System. *IEEE Internet of Things Journal*, 9(12): 9310-9319. <https://doi.org/10.1109/JIOT.2021.3130434>
- [5] Muthanna, M.S.A., Alkanhel, R., Muthanna, A., Rafiq, A., Abdullah, W.A.M. (2022). Towards SDN-enabled, intelligent Intrusion Detection System for Internet of Things (IoT). *IEEE Access*, 10: 22756-22768. <https://doi.org/10.1109/ACCESS.2022.3153716>
- [6] Mallikarjunaswamy, S., Basavaraju, N.M., Sharmila, N., Mahendra, H.N., Pooja, S., Deepak, B.L. (2022). An efficient big data gathering in wireless sensor network using reconfigurable node distribution algorithm. In *2022 Fourth International Conference on Cognitive Computing and Information Processing (CCIP)*, Bengaluru, India, pp. 1-6. <https://doi.org/10.1109/CCIP57447.2022.10058620>
- [7] Shankara, K.H., Srikantaswamy, M., Nagaraju, S. (2025). An efficient load-balancing in machine learning-based DC-DC conversion using renewable energy resources. *IAES International Journal of Artificial Intelligence*, 14(1): 307-316. <https://doi.org/10.11591/ijai.v14.i1.pp307-316>
- [8] Pushpalatha, V., Mallikarjuna, P.B., Mahendra, H.N., Subramoniam, S.R., Mallikarjunaswamy, S. (2025). Land use and land cover classification for change detection studies using convolutional neural network. *Applied Computing and Geosciences*, 25: 100227. <https://doi.org/10.1016/j.acags.2025.100227>
- [9] Poornima, M., Anitha, N., Mallikarjuna, S., Umashankar, L. (2025). An efficient internet of things based intrusion detection and optimization algorithm for smart networks. *International Journal of Computing and Digital Systems*, 17: 1-12. <https://doi.org/10.12785/ijcds/1571001227>
- [10] Venkatesh, D.Y., Mallikarjunaiah, K., Srikantaswamy, M. (2025). Efficient reconfigurable parallel switching for low-density parity-check encoding and decoding. *IAES International Journal of Artificial Intelligence*, 14(1): 260-269. <https://doi.org/10.11591/ijai.v14.i1.pp260-269>
- [11] Sukumar, P.G., Krishnaiah, M., Velluri, R., Satish, P., Nagaraju, S., Puttaswamy, N.G., Srikantaswamy, M. (2024). An efficient adaptive reconfigurable routing protocol for optimized data packet distribution in network on chips. *International Journal of Electrical and Computer Engineering*, 14(1): 305-314. <https://doi.org/10.11591/ijece.v14i1.pp305-314>
- [12] Kumar, S.M., Velluri, R., Dayananda, P., Nagaraj, S., Srikantaswamy, M., Chandrappa, K.Y. (2023). An efficient detection and prediction of intrusion in smart grids using artificial neural networks. *International Conference on Data Science, Computation and Security*, pp. 505-515. https://doi.org/10.1007/978-981-97-0975-5_45
- [13] Kumar, S.M., Nagaraj, S., Veerabhadraswamy, P., Nanjundaswamy, M.H., Srikantaswamy, M., Chandratta, K.Y. (2023). An enhanced power management and prediction for smart grid using machine learning. *International Conference on Data Science, Computation and Security*, pp. 269-277. https://doi.org/10.1007/978-981-97-0975-5_24
- [14] Shankara, K.H., Srikantaswamy, M., Nagaraju, S. (2024). A comprehensive study on DC-DC converter for equal

- current sharing and voltage stability in renewable energy resources. *Journal Européen des Systèmes Automatisés*, 57(2): 323-334. <https://doi.org/10.18280/jesa.570202>
- [15] Honnegowda, J., Mallikarjunaiah, K., Srikantaswamy, M. (2024). An efficient abnormal event detection system in video surveillance using deep learning-based reconfigurable autoencoder. *Ingénierie des Systèmes d'Information*, 29(2): 677-686. <https://doi.org/10.18280/isi.290229>
- [16] Jyothi, H., Komala, M., Mallikarjunaswamy, S. (2024). A comprehensive survey on technologies in video-based event detection and recognition using machine learning and deep learning techniques. In *2024 Second International Conference on Networks, Multimedia and Information Technology (NMITCON)*, Bengaluru, India, pp. 1-5. <https://doi.org/10.1109/NMITCON62075.2024.10698959>
- [17] Basavaraju, N.M., Mahadevaswamy, U.B., Mallikarjunaswamy, S. (2024). Design and implementation of crop yield prediction and fertilizer utilization using iot and machine learning in smart agriculture systems. In *2024 Second International Conference on Networks, Multimedia and Information Technology (NMITCON)*, Bengaluru, India, pp. 1-6. <https://doi.org/10.1109/NMITCON62075.2024.10699184>
- [18] Kavya, B.M., Mallikarjunaswamy, S., Sharmila, N., Shilpa, M., et al. (2024). An efficient machine learning-based power management system for smart grids using renewable energy resources. In *2024 Second International Conference on Networks, Multimedia and Information Technology (NMITCON)*, Bengaluru, India, pp. 1-7. <https://doi.org/10.1109/NMITCON62075.2024.10698819>
- [19] Alani, M.M., Awad, A.I. (2023). An intelligent two-layer Intrusion Detection System for the Internet of Things. *IEEE Transactions on Industrial Informatics*, 19(1): 683-692. <https://doi.org/10.1109/TII.2022.3192035>
- [20] Cui, J., Sun, H., Zhong, H., Zhang, J., Wei, L., Bolodurina, I., He, D. (2023). Collaborative Intrusion Detection System for SDVN: A fairness federated deep learning approach. *IEEE Transactions on Parallel and Distributed Systems*, 34(9): 2512-2528. <https://doi.org/10.1109/TPDS.2023.3290650>
- [21] Jadagerimath, A.N., Mallikarjunaswamy, S., Kumar, M., Sheela, S., Prakash, S., Tevaramani, S.S. (2023). A machine learning based consumer power management system using smart grid. In *2023 International Conference on Recent Advances in Science and Engineering Technology (ICRASET)*, B G Nagara, India, pp. 1-5. <https://doi.org/10.1109/ICRASET59632.2023.10419979>
- [22] Charitha, M., Hosur, S., Srikantaswamy, M. (2025). Optimized BER reduction in wireless communication using a chaos-based CDSK modulation model. *Mathematical Modelling of Engineering Problems*, 12(2): 719-729. <https://doi.org/10.18280/mmep.120234>
- [23] Jyothi, S., Mallikarjunaswamy, S., Kavitha, M., Sharmila, N., Kavya, B.M. (2023). A machine learning based power load prediction system for smart grid energy management. In *2023 International Conference on Recent Advances in Science and Engineering Technology (ICRASET)*, B G Nagara, India, pp. 1-6. <https://doi.org/10.1109/ICRASET59632.2023.10420183>
- [24] Rullo, A., Midi, D., Mudjerikar, A., Bertino, E. (2024). Kalis2.0—A SECaaS-based context-aware self-adaptive Intrusion Detection System for IoT. *IEEE Internet of Things Journal*, 11(7): 12579-12601. <https://doi.org/10.1109/JIOT.2023.3333948>
- [25] Al-Hamadi, H., Chen, I.R., Wang, D.C., Almashan, M. (2020). Attack and defense strategies for intrusion detection in autonomous distributed IoT systems. *IEEE Access*, 8: 168994-169009. <https://doi.org/10.1109/ACCESS.2020.3023616>
- [26] Wei, N., Yin, L., Tan, J., Ruan, C., Yin, C., Sun, Z., Luo, X. (2023). An autoencoder-based hybrid detection model for intrusion detection with small-sample problem. *IEEE Transactions on Network and Service Management*, 21(2): 2402-2412. <https://doi.org/10.1109/TNSM.2023.3334028>
- [27] Alsaedi, A., Moustafa, N., Tari, Z., Mahmood, A., Anwar, A. (2020). TON_IoT telemetry dataset: A new generation dataset of IoT and IIoT for data-driven Intrusion Detection Systems. *IEEE Access*, 8: 165130-165150. <https://doi.org/10.1109/ACCESS.2020.3022862>
- [28] Umashankar, M.L., Mallikarjunaswamy, S., Sharmila, N., Kumar, D.M., Nataraj, K.R. (2023). A survey on IoT protocol in real-time applications and its architectures. In *ICDSMLA 2021: Proceedings of the 3rd International Conference on Data Science, Machine Learning and Applications*. Singapore: Springer, pp. 119-130. https://doi.org/10.1007/978-981-19-5936-3_12
- [29] Liu, J., Yang, D., Lian, M., Li, M. (2021). Research on intrusion detection based on particle swarm optimization in IoT. *IEEE Access*, 9: 38254-38268. <https://doi.org/10.1109/ACCESS.2021.3063671>
- [30] Kamaldeep, Malik, M., Dutta, M., Granjal, J. (2021). IoT-Sentry: A cross-layer-based Intrusion Detection System in standardized Internet of Things. *IEEE Sensors Journal*, 21(24): 28066-28076. <https://doi.org/10.1109/JSEN.2021.3124886>
- [31] Nallakuruppan, M.K., Somayaji, S.R.K., Fuladi, S., Benedetto, F., Ulaganathan, S.K., Yenduri, G. (2024). Enhancing security of host-based Intrusion Detection Systems for the Internet of Things. *IEEE Access*, 12: 31788-31797. <https://doi.org/10.1109/ACCESS.2024.3355794>
- [32] Wardhani, R.W., Putranto, D.S.C., Jo, U., Kim, H. (2023). Toward enhanced attack detection and explanation in Intrusion Detection System-based IoT environment data. *IEEE Access*, 11: 131661-131676. <https://doi.org/10.1109/ACCESS.2023.3336678>
- [33] Oseni, A., Moustafa, N., Creech, G., Sohrabi, N., Strelzoff, A., Tari, Z., Linkov, I. (2022). An explainable deep learning framework for resilient intrusion detection in IoT-enabled transportation networks. *IEEE Transactions on Intelligent Transportation Systems*, 24(1): 1000-1014. <https://doi.org/10.1109/TITS.2022.3188671>
- [34] Khan, N., Khan, S.U., Ullah, F.U.M., Lee, M.Y., Baik, S.W. (2023). AI-assisted hybrid approach for energy management in IoT-based smart microgrid. *IEEE Internet of Things Journal*, 10(21): 18861-18875. <https://doi.org/10.1109/JIOT.2023.3293800>
- [35] Kavitha, H.S., Mallikarjunaswamy, S., Sharmila, N.

(2024). An optimized power management system for solar and wind energy using hybrid inverters and machine learning. In 2024 Second International Conference on Networks, Multimedia and Information Technology (NMITCON), Bengaluru, India, pp. 1-6. <https://doi.org/10.1109/NMITCON62075.2024.10698831>

[36] Kavitha, H.S., Usha, S.M., Sheela, S.N., Anu, H., et al.

(2024). Optimized crop prediction and monitoring using ensemble machine learning algorithms. In 2024 Second International Conference on Networks, Multimedia and Information Technology (NMITCON), Bengaluru, India, pp. 1-6. <https://doi.org/10.1109/NMITCON62075.2024.10698915>