Received: March 22, 2024. Revised: July 13, 2024.

INASS

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

HIDE-6G: Advanced Intrusion Detection System for Secure 6G Network using Deep Learning

Mamidipaka Hema[1]* Gurunadha. R[1] Neelima. A[2] Muthukumaran. N[3]
Geetha. A[4] Manjula. S[5]

[1]*Department of Electronics and Communication Engineering,*
JNTUGVCEV College of Engineering, Vizianagaram, Andhra Pradesh , India
[2]*Computer Science and Engineering, SRKR Engineering College(A), Bhimavaram, Andhra Pradesh 534204, India*
[3]*Centre for Computational Imaging and Machine Vision, Department of Electrical and Computer Engineering,*
Sri Eshwar College of Engineering, Coimbatore – 641202, Tamil Nadu, India
[4]*Department of Electrical and Electronics Engineering,*
P. S. R Engineering college, Sivakasi, Tamil Nadu – 626140, India
[5]*Department of Computer Science and Engineering,*
Ramco Institute of Technology, Rajapalayam, Tamil Nadu, India
* Corresponding author's Email: mhema.ece@jntugvcev.edu.in

Abstract: Sixth-generation (6G) wireless networks are anticipated to undergo trials and installations as early as 2030, offering unprecedented capacity, dependability, and efficiency. However, attention is shifting towards the development of 6G networks to meet the demands of emerging applications. The transition to 6G brings new challenges, particularly in the realm of intrusion detection, where the sophistication of attacks necessitates advanced security solutions. To eliminate this challenge, a novel Hybrid Intrusion DEtection system for the 6G network (HIDE-6G) has been proposed to detect intrusion in the 6G network. The proposed method leverages advanced techniques such as Principal Component Analysis (PCA) for dimensionality reduction, a Spotted Hyena Optimization Algorithm for feature selection, and a Capsule Network-based Deep Autoencoder (CapsDA) for effective anomaly detection. The performance of the HIDE-6G is estimated using the NSL-KDD and CICIDS 2019 datasets, demonstrating superior results compared to existing techniques such as AD6GN, IDSoft, and LA-HLRW. According to the comparison analysis, the proposed HIDE-6G technique's detection rate is 6.10%, 22.27%, and 20.7% greater than the existing HADES-IoT, H3SC-DLIDS, and F-BIDS techniques respectively.

Keywords: 6G network, Intrusion detection, Capsule network-based deep autoencoder, Deep learning, Spotted hyena optimization.

1. Introduction

5G network infrastructure deployment has already started, and in the upcoming years, a widespread expansion is anticipated [1]. To meet the demands of applications for the upcoming ten years, academia and industry are presently concentrating on 6G [2]. Several instances demonstrate how 5G networks are limited in terms of data rate, latency, coverage worldwide, and other aspects [3]. The potential of 6G network infrastructures will be fully realized by emerging applications like digital twin technologies, holographic communications, and extended reality [4]. The key benefits of 6G over 5G networks are their high data throughput, energy efficiency, low latency, and widespread device connectivity [5].

Zero-day attack detection is a challenging problem because suspicious activity is found every day. These sophisticated intrusions can have serious consequences that increase the difficulty for existing intrusion detection systems (IDSs) [6-8]. When they detect unexpected activity or a known threat, IDSs

issue alerts. They look for indications of potentially dangerous conduct, network packets conveying unauthorized access to the system, and cyber resistance against disruptive activities [9].

In 6G networks, an intrusion detection system aims to detect unusual patterns in network traffic, act quickly to stop security breaches, and monitor network traffic proactively [10-12].

Recent years have seen the emergence of numerous advanced optimization algorithms, such as Extended Stochastic Coati Optimizer [13], Swarm Bipolar Algorithm [14], Four Directed Search Algorithm [15], Total Interaction Algorithm [16], Walk-Spread Algorithm [17], and Attack Leave Optimizer [18]. Each of these algorithms offers distinct strengths and applications. However, it's essential to recognize that the choice of optimization algorithm should align with the specific problem being addressed. While newer algorithms often boast improved performance, they may not necessarily outperform older ones in every scenario. In the case of the SHO, its utilization might be justified by its unique ability to mimic the cooperative hunting behavior of spotted hyenas, which can be advantageous in feature selection.

Due to the increased intricacy and interconnectivity of 6G networks, intrusion detection systems may find it difficult to quickly and accurately detect and neutralize sophisticated and advanced cyber threats [19,20]. To overcome these issues a novel Hybrid Intrusion DEtection system for 6G network (HIDE-6G) has been proposed. The main contributions of the proposed method are as follows:

- Initially, the data are gathered from the 6G base station and the data includes normal profile data, which is the information about the users and their devices, and packet traffic data.
- The collected data are pre-processed using data cleaning and data transformation steps to make the data suitable for further analysis.
- From the preprocessed data, the data are extracted using the PCA technique. The most important and relevant features of data are selected using the SHO Algorithm to find the best features that can differentiate between normal and attack data.
- Finally, the selected features are given as input to the CapsDA model for further classification. The output is classified into 2 classes such as attack detected and no attack detected.

The following explanation pertains to the remaining half of this research: In Section II, the research is examined concerning the literature. Section III provides a detailed explanation of the suggested system. The conclusion is found in Section V, whereas the result and discussion are found in Section IV.

2. Literature survey

In current years, an amount of studies have used a variety of methodologies to identify the vulnerabilities in 6G networks. A number of the contemporary evaluation techniques are discussed in the part that follows, along with some of their drawbacks:

In 2021, Zhang, Z., et al., [21] created a special weight-based ensemble machine learning algorithm (WBELA) to detect aberrant signals from the car Controller Area Network (CAN) bus system. The outcomes of the experiments show that the suggested approaches outperform existing methods about performance, correctness, and false positive rate. One potential disadvantage of this approach is its reliance on simulated data for evaluation rather than real-world data.

In 2022, Farooq, M. and Khan, M.H., [22] suggested a key for a wireless 6G IoT network invasion discovery method based on signatures. In wireless 6G IoT networks, security is measured by an IDS that is based on signatures. This produced a 98.9% accuracy rate after three distinct methods One disadvantage of using a signature-based IDS in wireless 6G IoT networks is its limitation in detecting unknown or zero-day attacks

In 2023, Saeed, M.M., et al., [23] suggested a brand-new EL based anomaly detection system for 6G networks (AD6GNs) for communication networks. Notably, NSL_KDD had 99.5% accuracy (false alarm rate: 0.0038), UNSW_NB2015 had 99.9% accuracy (false alarm rate: 0.0076), CIC_IDS2017 had 99.8% accuracy (false alarm rate: 0.0009), and CICDDOS2019 had 99.95426% accuracy (false alarm rate: 0.00113). One potential disadvantage of the proposed method is its reliance on historical data for training.

In 2023, Alotaibi, A. and Barnawi, A., [24] suggested a brand-new, cutting-edge security architecture known as IDSoft, which stands for NextGen IDS. The numerical findings show that the suggested HFL method promises higher scalability, speeds convergence, and dramatically decreases communication overhead. The limitation of the suggested IDSoft solution is the increased complexity and potential vulnerabilities introduced by softwarization.

In 2023, Bhuvaneshwari, B., et al., [25] suggested a technique for 6G attack detection known as Luong

Attention and Hosmer Lem show Regression Window-based (LA-HLRW). In addition to improving attack detection accuracy, the total study of the proposed LA-HLRW results showed a significant 24% reduction in attack detection time. The suggested method's complexity may increase the maintenance burden, requiring ongoing efforts to ensure the IDS remains effective over time.

In 2024, Kusuma, P.D. and Kallista, M., [27] suggested the migration-crossover algorithm (MCA), a revolutionary swarm-based metaheuristic. The midpoint of two randomly chosen solutions is key in fixed dimension functions, while the global finest solution takes precedence in high dimension functions. According to the outcome, MCA is finer in 20, 19, 17, 20, and 17 functions thereafter than TIA, OOA, MA, COA, and WaOA.

In 2024, Kusuma, P.D. and Kallista, M., [28] presented a unique metaheuristic, the swarm space hopping algorithm (SSHA), This work evaluates the performance of SSHA through three assessments. The outcome demonstrates that SSHA outperforms NGO, ZOA, CLO, OOA, and TIA in functions 21, 20, 17, 17, and 21, and that the third search's contribution is only meaningful in three of these functions.

Several investigations have probed security vulnerabilities in 6G networks. Yet, existing approaches suffer from reduced accuracy and increased latency. Our method stands out in its performance metrics like accuracy, false positive rate, detection time, and computational overhead and compared to prior literature. Highlighting these differences aims to underscore the novelty and effectiveness of our proposed methodology in addressing current limitations. The subsequent section discusses our unique approach to overcoming these drawbacks.

3. Hybrid intrusion detection system for 6g network (HIDE-6G)

In this section, a novel Hybrid Intrusion DEtection system for the 6G network (HIDE-6G) has been proposed to detect intrusion in the 6G network. Data is initially collected from the 6G base station, including normal profile data and packet traffic data. This collected data undergoes preprocessing steps

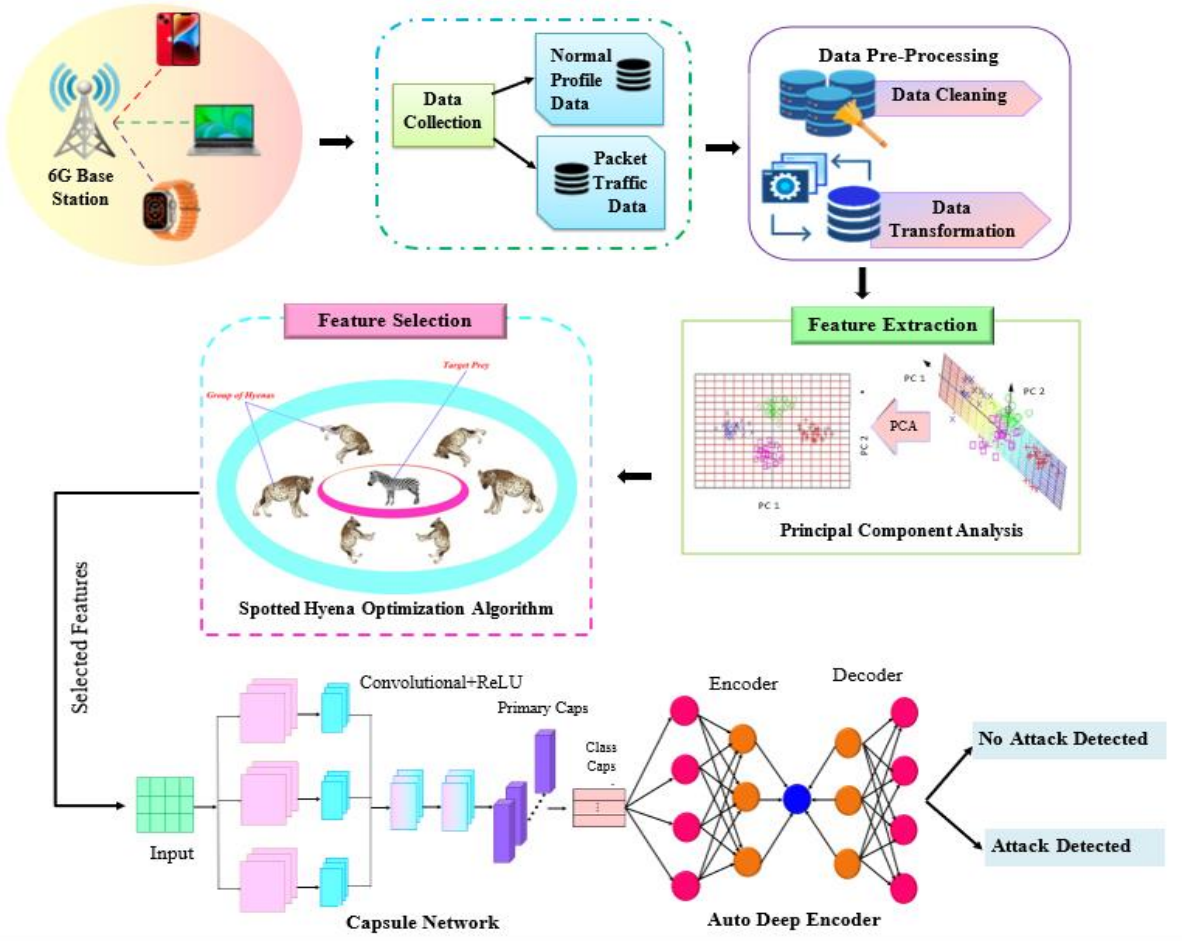


Figure. 1 The overall workflow of the Proposed HIDE-6G Method

involving data cleaning and transformation. PCA is then applied to reduce complexity and noise.Relevant features are selected using the SHO Algorithm, aimed at distinguishing between normal and attack data. These selected features are inputted into a CapsDA model for classification, resulting in two classes: attack detected or no attack detected. The proposed HIDE-6G method's whole framework is shown in Fig. 1.

3.1 Data collection

Data collection is an important step in the progression of intrusion detection using a deep learning model. It involves gathering two types of data from a 6G base station: normal profile data and packet traffic data.

3.2 Data pre-processing

Data pre-processing involves cleaning and transforming the collected data to make it suitable for feature extraction and selection.

3.2.1. Data cleaning

Data cleaning is vital for boosting accuracy in intrusion detection models for 6G networks. It involves identifying and rectifying data irregularities to ensure dataset reliability by addressing noise, outliers, and missing values. This improves the efficacy of security protocols by enabling better differentiation between hostile and legitimate network activity in the complex 6G environment.

3.2.2. Data transformation

Data transformation via normalization and scaling is essential for maximizing model performance in the field of intrusion detection for 6G networks. By making linear changes to the initial data, min-max normalization aims to produce a balance of value comparisons among the data before and after the process. Eq. (1) provides the formula that can be used with this strategy.

$$Z_{new} = \frac{Z - mn(Z)}{mx(Z) - \mathrm{mn}\ (Z)} \tag{1}$$

Where Z_{new} is the adjusted value derived from the normalized outcomes, Z denotes the previous value, after preprocessing using data cleaning and data transformation methods, the preprocessed data is given to the feature extraction module.

3.3 Feature extraction

The preprocessed data is subjected to feature extraction using the Principal Component Analysis approach.

3.3.1. Principal component analysis (PCA)

A popular method for reducing feature dimensionality is PCA. The algebraic definition of PCA is as follows, Calculate the mean of A for data framework A is given in Eq. (2) and Determine A's covariance is given in Eq. (3)

$$\delta = F(A) \tag{2}$$

$$CU = C_{ov}(A) = F[(A - \delta)(A - \delta)^T] \tag{3}$$

Where δ represents the result of the function F applied to matrix A. CU denotes the covariance matrix of matrix A, and C_{ov} represents the covariance operator. A is the original data matrix. The equation is solved for the Covariance CoV;

$$V_k = \frac{\sum_{i=1}^{L} \delta_n}{\sum_{i=1}^{M} \delta_n} \tag{4}$$

Where, δ_n denotes the n-th eigenvalue. L is the number of eigenvalues considered. M is the total number of eigenvalues. The mutual range should be 83% greater than the size of the major segments.

$$g = V^t - X \tag{5}$$

$$|\, \delta l - C0V| = 0 \tag{6}$$

Where X is the original data that was knotted, and t denotes the transfer matrix. l give the identity matrix credit for having dimensions that resemble CoV. The extracted features are given to the feature selection module to select the features.

3.4 Feature selection

Even with 6G networks, feature selection is an essential step in developing efficient IDS. SHO is used to pick features from the retrieved features.

3.4.1. Spotted hyena optimization (SHO)

The SHO mimics the community dynamics and hunting strategies of spotted hyenas with four stages, they are encircling, hunting, attacking prey, and searching. Fig. 2 shows the positional vectors of spotted hyenas in two dimensions.

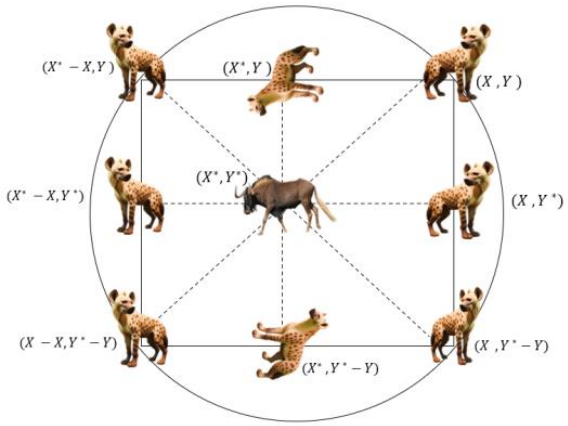


Figure. 2 Position vectors in two dimensions of spotted hyena

Encircling: When hunting in a group, hyenas attempt to get as near to their prey as they can to guide the group there. First, the most exceptional person in the group is recognized, and others adjust their opinions in line with that recognition. Eq. (7) models the encircling mechanism.

$$\overrightarrow{ds_h} = \left|\vec{X} \cdot \overrightarrow{Pt_{py}}(S) - \overrightarrow{Pt}(S)\right| \quad (7)$$

$$\overrightarrow{Pt}(S+1) = \overrightarrow{Pt_{py}}(S) - \vec{E} \cdot \overrightarrow{ds_h} \quad (8)$$

Where $\overrightarrow{ds_h}$ is the distance between a hyena and the location of its prey, $\overrightarrow{Pt}(S+1)$ is indicated by the hyena's novel location in the current repetition The symbol S represents the current iteration. $\overrightarrow{Pt_{py}}(S)$ denotes the position vector of the prey at iteration S.

$\overrightarrow{Pt}(S)$ signifies the current location of the hyena. Vector coefficients $\vec{X}$ and $\vec{E}$ are calculated by element-wise multiplication and position vectors in Eqs. (9) and (10).

$$\vec{X} = 2 \cdot \overrightarrow{rv_1} \quad (9)$$

$$\vec{E} = 2\vec{b} \cdot \overrightarrow{rv_2} - \vec{b} \quad (10)$$

$$\vec{b} = 5 - \left(i \times \left(\frac{5}{mx_i}\right)\right) \quad (11)$$

Eq. (11) indicates that $\vec{b}$ reduces linearly after 5 to 0 throughout the repetition and that $\overrightarrow{rv_1}$ and $\overrightarrow{rv_2}$ are accidental routes in the interval (0, 1).

Hunting: Hyenas are primarily social creatures that hunt in packs and have a good sense of where to find food. Eqs. (12) to (14), is used to determine which search agent is the best.

$$\overrightarrow{ds_h} = \left|\vec{X} \cdot \overrightarrow{Pt_h} - \overrightarrow{Pt_k}\right| \quad (12)$$

$$\overrightarrow{Pt_k} = \overrightarrow{Pt_h} - \vec{E}\,\overrightarrow{ds_h} \quad (13)$$

$$\overrightarrow{O_h} = \overrightarrow{Pt_k} + \overrightarrow{Pt_{k+1}} + \cdots + \overrightarrow{Pt_{k+N}} \quad (14)$$

Where, $\overrightarrow{Pt_h}$ determines the optimal placement of the first hyena, while $\overrightarrow{Pt_k}$ specifies the location of the additional hyenas. $\overrightarrow{O_h}$ is the cumulative search vector incorporating the positions of multiple hyenas. $\overrightarrow{Pt_k}, \overrightarrow{Pt_{k+1}}$ Position vectors of additional hyenas up to N. The number of hyenas is determined by using Eq. (15) and is shown in Parameter N.

$$N = count_{sol}\left(\overrightarrow{Pt_h} + \overrightarrow{Pt_{h+1}} + \overrightarrow{Pt_{h+2}}, \ldots\ldots, \left(\overrightarrow{Pt_h} + \vec{M}\right)\right) \quad (15)$$

Where $\vec{M}$ is an arbitrary route in the interval (0.5,1), and the $count_{sol}$ stricture in Eq. (15).

Attacking the Prey: The path h value is reduced to develop a scientific perfect for the intended bout. If the value of E in Eq. (16) is |E| < 1, the pack of uncontaminated hyenas is forced to bout the victim.

$$\overrightarrow{Pt}(S+1) = \frac{\overrightarrow{O_h}}{N} \quad (16)$$

The ideal position is saved and updated by $\overrightarrow{Pt}(S+1)$ in Eq. (16),

Finding prey: This strategy relies on altering the vector $\vec{E}$ to make hunting possible. $\vec{E}$ represents the arbitrary numbers that are greater than or less than −1.

A refined set of features are produced utilizing SHO.

3.5 Intrusion detection using capsule network-based deep auto encoder (CapsDA)

Intrusion Detection in 6G Networks employs a cutting-edge approach, utilizing a CapsDA. The architecture of the capsule network-based deep autoencoder is shown in Fig. 3.

3.5.1. Capsule network

CapsNet is a distinct neural network architecture that offers a simpler structure compared to CNN. Initially, the primary layer of the feature map is obtained by the capsule net architecture using 256, 9 x 9 complication kernels. Eq. (17) provides a summary of the procedure.

$$Y^{l+1}(r,s) = [Y^l \otimes \varphi^l](r,s) + a \quad (17)$$

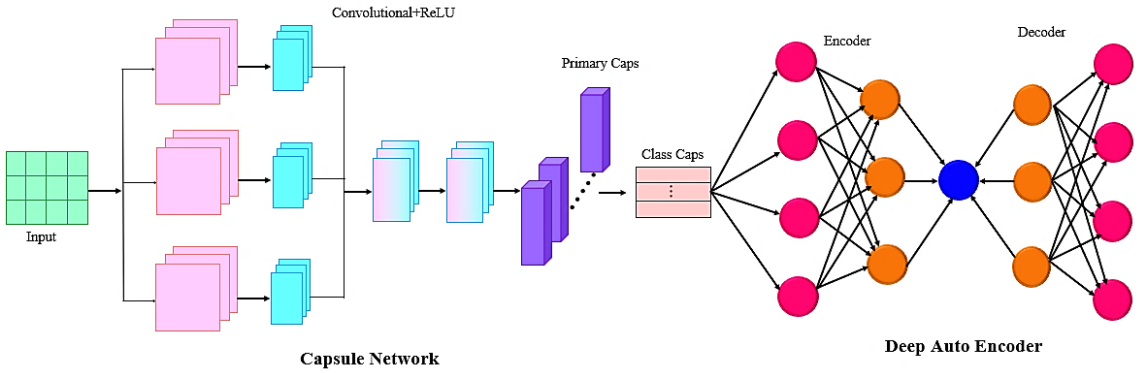


Figure. 3 The architecture of capsule network-based deep autoencoder

where a is the bias and $(r, s) \in \{0, 1, \ldots, Y^{l+1}\}$. Layer l+1's input and output are denoted by Y^l and Y^{l+1}.and $Y\ (r, s)$ is the corresponding pixel. Eq. (18) can be used to formalize the definition.

$$X_{i|j} = m_{i|j} \times v_j \tag{18}$$

Its initial logits a_{ji} represent the previous prospects that capsule j should be connected to capsule i, as illustrated in Eqs. (19) and (20).

$$o_{ji} = \frac{\exp\ (a_{ji})}{\sum_t b_{jt}} \tag{19}$$

$$s_i = \sum_j \left(o_{ji} \times X_{i|j}\right) \tag{20}$$

Here, o_{ji} represents the connection probability from capsule j to capsule i. a_{ji} is the initial logit. b_{jt} denotes the routing coefficients associated with capsule j for all possible connections Ultimately, it is only necessary to calculate $o_{j|i}$ instead of updating v_j, which can be expressed as Eqs. (21) and (22).

$$v_i = squash(sq_i) = \frac{||sq_i||^2}{1+||sq_i||^2} \times \frac{sq_i}{|sq_i|} \tag{21}$$

$$a_{j|i} = o_{j|i} + m_{j|i} \times v_j \tag{22}$$

Here, v_i is the Output after applying the squash function, $a_{j|i}$ is the Updated value for the target j based on input i. $o_{j|i}$ is the outcome for target j given input i.

3.5.2. Deep autoencoder

A deep autoencoder consists of an encoder and a decoder with multiple layers. The encoder maps input data EI to a lower-dimensional representation D, with the encoder function given in Eq. (23).

$$D = f_{enc}(EI) = \mu(wt_{enc}EI + a_{enc}) \tag{23}$$

Where μ is the activation function, D is the encoded representation, wt_{enc} is the mass medium, and a_{enc} is the bias vector. Eq. (24) can be used to express the decoder function.

$$EI' = f_{dec}(D) = \mu(wt_{dec}D + a_{dec}) \tag{24}$$

Here, the decoder weight matrix is wt_{dec}, and the decoder bias vector is a_{dec}. A final softmax layer is applied to classify the output into two classes: Attack Detected and No Attack Detected.

4. Results and discussion

In this section, the experimental results of the proposed HIDE-6G method are investigated, and performance is discussed in terms of multiple assessment metrics such as F1-Score, accuracy, false alarm rate, Precision, detection rate, security rate, latency and response time. The efficacy of the HIDE-6G is assessed with the use of NSL-KDD and CICIDS 2019 Datasets. The proposed HIDE-6G method have been compared to those of existing techniques, including AD6GN [23], IDSoft [24], and LA-HLRW [25]

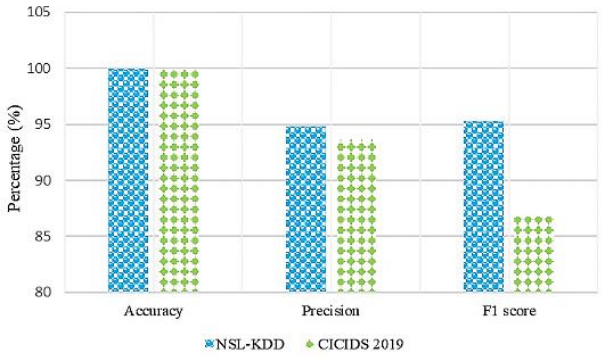
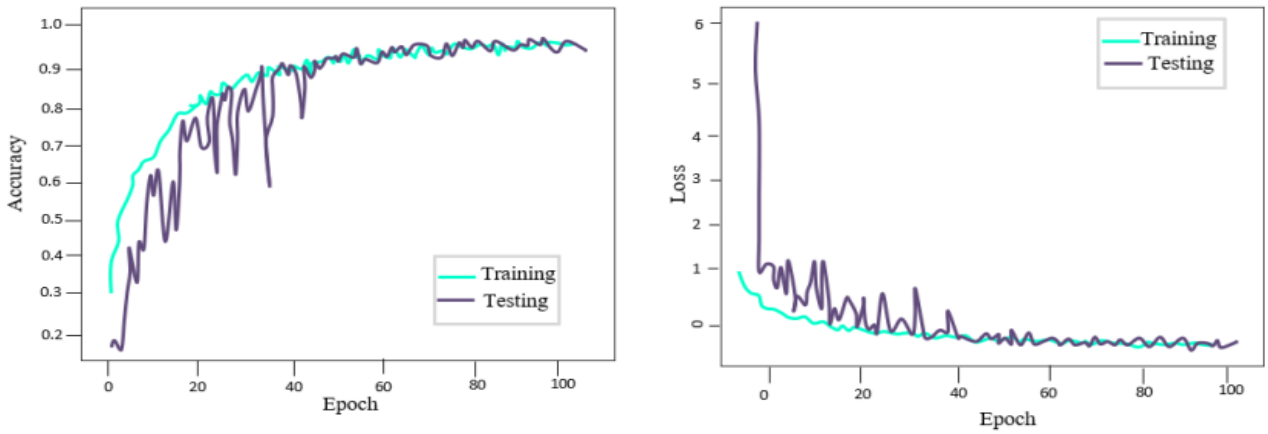


Figure. 4 Performance Comparison



(a) (b)

Figure. 5: (a) Accuracy Curve and (b) Loss Curve

4.1 Performance analysis

The accuracy, precision, and F1 score performance comparison between the NSL-KDD and CICIDS 2019 data sets is displayed in Fig. 4. The model's accuracy and precision are higher than those of the NSL-KDD dataset, as shown by the F1 scores, which are 99.96%, 94.8%, and 95.3%, respectively.

Figs. 5 (a) and 5 (b) show the training and test data sets, as well as the accuracy and loss curves. The Accuracy Curve in 5 (a) shows how the model's accuracy increases on both the training and during training epochs.5 (b) shows a declining trend in both training and validation losses.

4.2 Comparative analysis

Fig. 6 compares the accuracy of the proposed HIDE-6G methodology with the existing methods, including AD6GN [23], IDSoft [24], and LA-HLRW [25] using the 2 datasets. The accuracy of the proposed system increases by 15.75%, 26.57%, and 14.6% when compared to the existing techniques.

Fig. 7 shows how the proposed HIDE-6G method compares to the existing AD6GN [23], IDSoft [24], and LA-HLRW [25] methodologies in terms of false alarm rate, based on datasets. The proposed HIDE-6G technique has a reduced false alarm rate than other existing techniques.

Fig. 8 presents a performance comparison of the detection rate for the proposed HIDE-6G technique and existing methods, using the datasets. Compared to the existing LA-HLRW, IDSoft, and AD6GN techniques, the detection rate increases by 6.10%, 22.27%, and 20.7% more than the proposed HIDE-6G method.

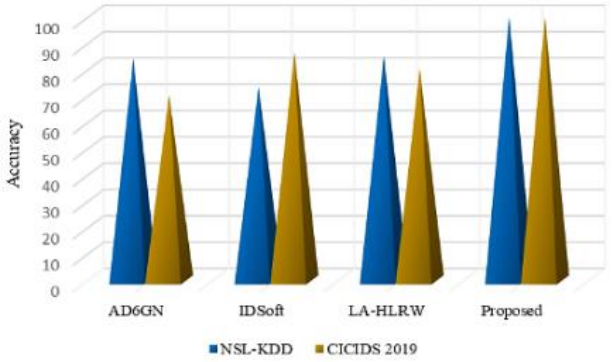


Figure. 6 Performance comparison in terms of accuracy

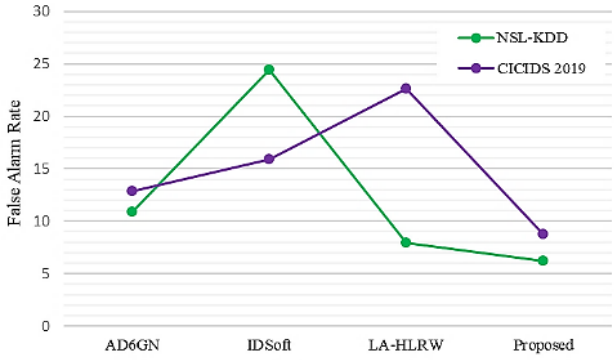


Figure. 7 Comparison in terms of False alarm rate

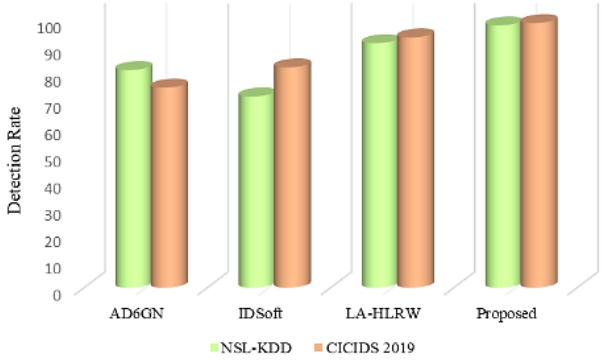


Figure. 8 Comparison in terms of detection rate

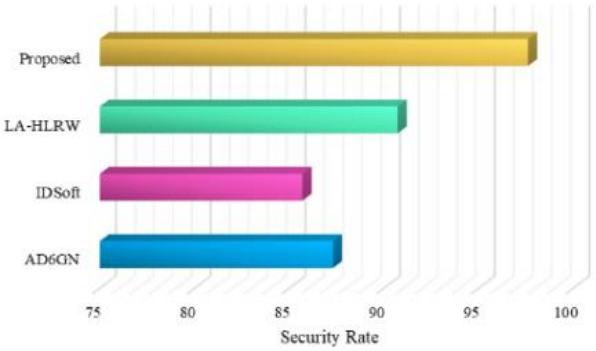


Figure. 9 Comparison in terms of security rate

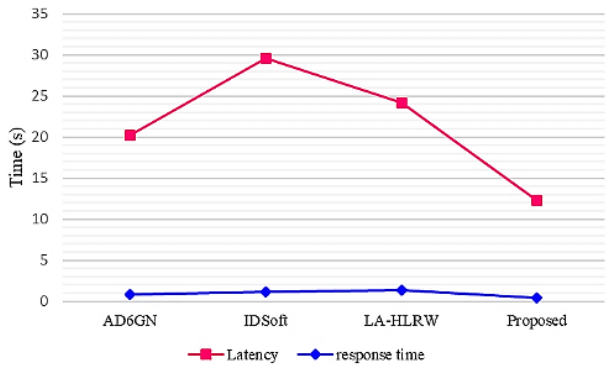


Figure. 10 Comparison in terms of latency and response time

Fig. 9. compares security rates of recommended and available intrusion detection approaches. The graphic illustrates each strategy's effectiveness in safeguarding systems. The security rate of proposed method is higher than the other existing methods.

Fig. 10 presents a comparison of latency and response time for both existing AD6GN [23], IDSoft [24], and LA-HLRW [25] and the proposed HIDE-6G method. Lower values indicate better efficiency.

5. Conclusion

In this paper, a novel Hybrid Intrusion DEtection system for the 6G network (HIDE-6G) has been proposed to detect intrusion in the 6G network. The incorporation of innovative techniques such as PCA for dimensionality reduction and the SHO for feature selection adds sophistication to the intrusion detection process. Additionally, the integration of CapsDA enables nuanced pattern learning for effective anomaly detection. The experimental results are based on evaluations using NSL-KDD and CICIDS 2019 datasets. The proposed HIDE-6G model's effectiveness is contrasted with existing technique in terms of F1-Score, accuracy, false alarm rate, Precision, detection rate, security rate, latency and response time. The proposed HIDE-6G method has a higher detection rate (6.10%, 22.27%, and 20.7%) than the current LA-HLRW, IDSoft, and AD6GN strategies. Future work will concentrate on adding real-time threat information inputs to the model to increase its awareness of the latest security threats.

Conflicts of Interest

This paper has no conflict of interest for publishing.

Author Contributions

The following statements should be used as follows: “Conceptualization, Mamidipaka Hema and Ravva Gurunadha; methodology, Neelima. A; software, Muthukumaran. N; validation, Geetha. A, and Mamidipaka Hema; formal analysis, Ravva Gurunadha; investigation, Neelima. A; resources, Muthukumaran. N; data curation, Geetha. A; writing original draft preparation, Mamidipaka Hema; writing review and editing, Neelima. A; visualization, Ravva Gurunadha; supervision, Muthukumaran. N; project administration, Geetha. A; funding acquisition, Mamidipaka Hema”, etc. Authorship must be limited to those who have contributed substantially to the work reported.

Acknowledgments

The author would like to express his heartfelt gratitude to the supervisor for his guidance and unwavering support during this research for his guidance and support.

Notations lists:

Notation	Definition
Z_{new}	Adjusted value derived from normalized outcomes
$mx(Z)$	Highest possible value
$mn\ (Z)$	Lowest possible number
CU	Covariance matrix of matrix A,
C_{ov}	The covariance operator
A	Original data matrix
δ_n	n-th eigenvalue
L	Number of eigenvalues considered
M	Total number of eigenvalues
X	Original data that was knotted
$\overrightarrow{ds_h}$	Distance amid a hyena and location of its prey
$\overrightarrow{Pt}(S+1)$	Hyena's novel location in the current repetition
$\overrightarrow{Pt_{py}}(S)$	Position vector of the prey at iteration S
$\overrightarrow{Pt}(S)$	Current position of the hyena
$\overrightarrow{Pt_h}$	Optimal placement of the first hyena,
$\vec{M}$	arbitrary route in the interval (0.5,1)

$\overrightarrow{O_h}$	Cumulative search vector incorporating the positions of multiple hyenas

References

[1] I. F. Akyildiz, S. Nie, S. C. Lin, and M. Chandrasekaran, "5G roadmap: 10 key enabling technologies", *Computer Networks*, Vol. 106, pp. 17-48, 2016.

[2] W. Jiang, B. Han, M. A. Habibi, and H. D. Schotten, "The road towards 6G: A comprehensive survey", *IEEE Open Journal of the Communications Society*, Vol. 2, pp. 334-366, 2021.

[3] N. Al-Falahy, and O. Y. Alani, "Technologies for 5G networks: Challenges and opportunities", *It Professional*, Vol. 19, No. 1, pp.12-20, 2017.

[4] Y. Lu, and X. Zheng, "6G: A survey on technologies, scenarios, challenges, and the related issues", *Journal of Industrial Information Integration*, Vol. 19, pp. 100158, 2020.

[5] F. Salahdine, T. Han, and N. Zhang, "5G, 6G, and Beyond: Recent advances and future challenges", *Annals of Telecommunications*, Vol. 78, No. 9, pp. 525-549, 2023.

[6] R. Ahmad, I. Alsmadi, W. Alhamdani, and L. A. Tawalbeh, "Zero-day attack detection: a systematic literature review", *Artificial Intelligence Review*, Vol. 56, No. 10, pp.10733-10811, 2023.

[7] C. V. Zhou, C. Leckie, and S. Karunasekera, "A survey of coordinated attacks and collaborative intrusion detection", *Computers & Security*, Vol. 29, No. 1, pp.124-140, 2010.

[8] R. Makwana, "IDS for Internet of things (IoT) and Industrial IoT Network", *Artificial Intelligence for Intrusion Detection Systems*, pp. 117-132, 2023.

[9] M. Z. Gunduz, and R. Das, "Cyber-security on smart grid: Threats and potential solutions", *Computer Networks*, Vol. 169, pp. 107094, 2020.

[10] A. Alotaibi, and A. Barnawi, "Securing massive IoT in 6G: Recent solutions, architectures, future directions", *Internet of Things*, Vol. 22, pp. 100715, 2023.

[11] J. Bharadiya, "Machine learning in cybersecurity: Techniques and challenges", *European Journal of Technology*, Vol. 7, No. 2, pp.1-14, 2023.

[12] J. R. Bhat, and S. A. Alqahtani, "6G ecosystem: Current status and future perspective", *IEEE Access*, Vol. 9, pp.43134-43167, 2021.

[13] P. D. Kusuma, and A. Dinimaharawati, "Extended stochastic coati optimizer", *International Journal of Intelligent Engineering and Systems*, Vol. 16, No. 3, pp. 482-494, 2023, doi: 10.22266/ijies2023.0630.38.

[14] P. D. Kusuma, and A. Dinimaharawati, "Swarm Bipolar Algorithm: A Metaheuristic Based on Polarization of Two Equal Size Sub Swarms", *International Journal of Intelligent Engineering & Systems*, Vol. 17, No. 2, 2024, doi: 10.22266/ijies2024.0430.31.

[15] P. D. Kusuma, and A. Dinimaharawati, "Four Directed Search Algorithm: A New Optimization Method and Its Hyper Strategy Investigation", *International Journal of Intelligent Engineering & Systems*, Vol. 16, No. 5, 2023, doi: 10.22266/ijies2023.1031.51.

[16] P. D. Kusuma, and A. Novianty, "Total Interaction Algorithm: A Metaheuristic in which Each Agent Interacts with All Other Agents", *International Journal of Intelligent Engineering & Systems*, Vol. 16, No. 1, 2023, doi: 10.22266/ijies2023.0228.20.

[17] P. D. Kusuma, and A. L. Prasasti, "Walk-Spread Algorithm: A Fast and Superior Stochastic Optimization", *International Journal of Intelligent Engineering & Systems*, Vol. 16, No. 5, 2023, doi: 10.22266/ijies2023.1031.24.

[18] P. D. Kusuma, and F. C. Hasibuan, "Attack-Leave Optimizer: A New Metaheuristic that Focuses on The Guided Search and Performs Random Search as Alternative", *International Journal of Intelligent Engineering & Systems*, Vol. 16, No. 3, 2023, doi: 10.22266/ijies2023.0630.19.

[19] M. Banafaa, I. Shayea, J. Din, M. H. Azmi, A. Alashbi, Y. I. Daradkeh, and A. Alhammadi, "6G mobile communication technology: Requirements, targets, applications, challenges, advantages, and opportunities", *Alexandria Engineering Journal*, Vol. 64, pp. 245-274, 2023.

[20] N. Perry, and S. Bhunia, "Crossfire Attack Detection in 6G Networks with the Internet of Things (IoT)", In: *Proc. of IFIP International Internet of Things Conf*, pp. 272-289, 2023.

[21] Z. Zhang, Y. Cao, Z. Cui, W. Zhang, and J. Chen, "A many-objective optimization based intelligent intrusion detection algorithm for enhancing security of vehicular networks in 6G", *IEEE Transactions on Vehicular Technology*, Vol. 70, No. 6, pp. 5234-5243, 2021.

[22] M. Farooq, and M. H. Khan, "Signature-Based Intrusion Detection System in Wireless 6G IoT

Networks", *Journal on Internet of Things*, Vol. 4, No. 3, 2022.
[23] M. M. Saeed, R. A. Saeed, M. Abdelhaq, R. Alsaqour, M. K. Hasan, and R. A. Mokhtar, "Anomaly detection in 6G networks using machine learning methods", *Electronics*, Vol. 12, No. 15, pp. 3300, 2023.
[24] A. Alotaibi, and A. Barnawi, "IDSoft: A federated and softwarized intrusion detection framework for massive internet of things in 6G network", *Journal of King Saud University-Computer and Information Sciences*, Vol. 35, No. 6, pp. 101575, 2023.
[25] B. Bhuvaneshwari, B. Balusamy, R. K. Dhanaraj, and V. Ravi, "Artificial intelligence enabled Luong Attention and Hosmer Lemeshow Regression Window-based attack detection in 6G", *International Journal of Communication Systems*, Vol. 36, No. 15, pp. e5571, 2023.
[26] P. D. Kusuma, and M. Kallista, "Migration-Crossover Algorithm: A Swarm-based Metaheuristic Enriched with Crossover Technique and Unbalanced Neighbourhood Search", *International Journal of Intelligent Engineering & Systems*, Vol. 17, No. 1, 2024, doi: 10.22266/ijies2024.0229.59.
[27] P. D. Kusuma, and M. Kallista, "Swarm Space Hopping Algorithm: A Swarm-based Stochastic Optimizer Enriched with Half Space Hopping Search", *International Journal of Intelligent Engineering & Systems*, Vol. 17, No. 2, 2024, doi: 10.22266/ijies2024.0430.54.