Journal of Applied Science

Biannual Peer Reviewed Journal Issued by Research and Consultation Center , Sabratha University

Issue (12)
April 2024

Journal of Applied Science

Biannual Peer Reviewed Journal Issued by Research and Consultation Center, Sabratha University

Editorial

We start this pioneering work, which do not seek perfection as much as aiming to provide a scientific window that opens a wide area for all the distinctive pens, both in the University of Sabratha or in other universities and research centers. This emerging scientific journal seeks to be a strong link to publish and disseminate the contributions of researchers and specialists in the fields of applied science from the results of their scientific research, to find their way to every interested reader, to share ideas, and to refine the hidden scientific talent, which is rich in educational institutions. No wonder that science is found only to be disseminated, to be heard, to be understood clearly in every time and place, and to extend the benefits of its applications to all, which is the main role of the University and its scholars and specialists. In this regard, the idea of issuing this scientific journal was the publication of the results of scientific research in the fields of applied science from medicine, engineering and basic sciences, and to be another building block of Sabratha University, which is distinguished among its peers from the old universities.

As the first issue of this journal, which is marked by the Journal of Applied Science, the editorial board considered it to be distinguished in content, format, text and appearance, in a manner worthy of all the level of its distinguished authors and readers.

In conclusion, we would like to thank all those who contributed to bring out this effort to the public. Those who lit a candle in the way of science which is paved by humans since the dawn of creation with their ambitions, sacrifices and struggle in order to reach the truth transmitted by God in the universe. Hence, no other means for the humankind to reach any goals except through research, inquiry, reasoning and comparison.

Editorial Committee

Notice

The articles published in this journal reflect the opinions of their authors only. They are solely bearing the legal and moral responsibility for their ideas and opinions. The journal is not held responsible for any of that.

Publications are arranged according to technical considerations, which do not reflect the value of such articles or the level of their authors.

Journal Address:

Center for Research and Consultations, Sabratha University

Website: **https://jas.sabu.edu.ly/index.php/asjsu**

Email**:** **jas@sabu.edu.ly**

Local Registration No. (435/2018)

ISSN 💻 2708-7301

ISSN 🕮 2708-7298

Publication instructions

The journal publishes high quality original researches in the fields of Pure Science, Engineering and Medicine. The papers can be submitted in English or Arabic language through the Journal email (jas@sabu.edu.ly) or CD. The article field should be specified and should not exceed 15 pages in single column.

All submitted research manuscripts must follow the following pattern:

- Title, max. 120 characters.
- Author Name, Affiliation and Email
- Abstract, max. 200 words.
- Keywords, max. 5 words.
- Introduction.
- Methodology.
- Results and Discussion.
- Conclusion.
- Acknowledgments (optional).
- References.

Writing Instructions:

Papers are to be submitted in A4 (200×285 mm) with margins of 25 mm all sides except the left side, which should be 30 mm. Line spacing, should also be 1.15.

Table 1. Font size and style

	Bold	English	Arabic
Font Style	✓	Times New Roman	Simplified Arabic
Article Title	✓	14 Capital	16
Authors Name	✓	12	14
Affiliation	×	11	13
Titles	✓	12	14
Sub-Title	✓	12	13
Text	×	12	14
Figure Title	✓	11	13
Table Title	✓	11	13
Equations	✓	12	14

Figures:

All figures should be compatible with Microsoft Word with serial numerals. Leave a space between figures or tables and text.

References:

The references should be cited as Harvard method, eg. Smith, R. (2006). References should be listed as follows:

Articles: Author(s) name, Year, Article Title, Journal Name, Volume and Pages.

Books: Author(s) name. Year. “Book title" Location: publishing company, pp.

Conference Proceedings Articles: Author(s) name. Year." Article title". Conference proceedings. pp.

Theses: Author(s) name. Year. "Title". Degree level, School and Location.

Invitation

The Editorial Committee invites all researchers "Lectures, Students, Engineers at Industrial Fields" to submit their research work to be published in the Journal. The main fields targeted by the Journal are:

- Basic Science.
- Medical Science & Technology.
- Engineering.

Refereeing

The Editorial Committee delivers researches to two specialized referees, in case of different opinions of arbitrators the research will be delivered to a third referee.

Editorial Committee

CONTENTS

ENERGY-EFFICIENT INTRUSION DETECTION IN WSN: LEVERAGING IK-ECC AND SA-BILSTM

Sana Abouljam[1] **and Anesa Al-Najeh**[2*]

[1] Department of Computer, Faculty of Science, Alajelat, Zawia University, Sabratha, Libya
[2] Department of Computer, Faculty of Science, Sabratha, Sabratha University, Sabratha, Libya
[*] anesa.alnajeh@sabu.edu.ly

Abstract

Wireless Sensor Networks (WSNs) play a vital role in numerous applications. This paper proposes an energy-efficient intrusion detection framework for WSNs. Initially, nodes are registered to the network. During registration a unique key is generated for each node. Then, the nodes are formed into cluster and for each cluster CH and SCH are selected. Thereafter, the path is created between the clustered nodes and the CH. After that, data transmission begins. To attain secure data transmission, the unique signature is generated for each data using RS-ECDSA and then the data is encrypted by IK-ECC. The encrypted data is transmitted to the sink node (SN), which acts as the gateway to base station (BS). In the SN, subnet masking and batch verification is performed. After that, IDS using Bi-LSTM is employed this predicts whether the data is attacked or not. The experimental result stated that the proposed method withstands energy efficient as compared to existing methodologies.

Keywords: Smish Activated-Bidirectional-Long Short Term Memory (SA-BilSTM); Identity-Key-based Elliptic Curve Cryptography (IK-ECC); Ring Sign-based Elliptic Curve Digital Signature Algorithm (RS-ECDSA); Skew Tent-based K-means (ST-KM); False Alarm rate (FAR).

Introduction

Wireless sensor network (WSN) plays a predominant role in household equipment to military applications (Basha, 2020). But, due to the widespread growth and propagation of network connectivity, the security requirement of WSN is ever-growing (Dwivedi et al., 2021). Thus, the effective IDS is treated as a solution to resolve the security issues in WSNs (Prithi & Sumathi, 2020). The IDSs are responsible for monitoring hosts and networks, and responding to malicious actions, like jamming, eavesdropping, back-hole, Sybil, and wormhole attacks (Hammad et al., 2020) (Ramadan, 2020). Recently, Deep Learning (DL) based IDSs have emerged as the leading systems in ID research domain (Kasongo & Sun, 2020). ML gives systems the ability to learn and improve by using previous data (Ahmad et al., 2021).

Meanwhile, WSNs have specific constraints, such as low energy efficiency that make the current IDSs challenging (Raiyat Aliabadi et al., 2021). As a result, designing an energy-efficient routing protocol is an utmost concern in extending the lifespan of the sensor node for WSN (Prithi & Sumathi, 2021). The clustering-based techniques, such as Low-energy adaptive clustering hierarchy (LEACH) (Fang et al., 2021) are focused to improve energy efficiency and to enhance security. But, such IDS models had the drawback of low detection accuracy and low network lifetime. To solve this, an energy-efficient IDS in WSN is proposed.

1. Problem Statement

Existing research problems,

- Security and energy issues arise when intruders try to attack the network by creating false alarms by varying the pattern of the packets.
- The IDS is developed for the recognition of intrusion based on features of the packets, which does not attempt to mitigate the intrusion.
- Single CH as the optimal source to transfer the data to the sink node is unreliable, as the CH might be in mobility or the energy might get drained.

2. Objectives

- To mitigate the false alarm rates and to avoid transmitting the data via spoofed sink node, the pattern verification is proposed.
- To detect and mitigate the attacks in WSN, the SA-LSTM and IK-ECC-based encryption of data are proposed.
- To improve energy efficiency, ST-K-mean clustering with the SCH with CH is selected.

The article is organized as; Section 2 describes the related works. Section 3 elaborates on the proposed methodology. Section 4 discusses the experimental outcomes. Finally, Section 5 concludes the paper.

Related Works

(Pan et al., 2021) developed a lightweight ID model for WSNs. The model combined the K-Nearest Neighbor (KNN) and Sine Cosine Algorithm (SCA) to detect a variety of attacks, including unknown attacks. This algorithm improved the energy-saving, and efficiency of ID. But, the space complexity of the KNN has increased the complexity of the model in real-time ID.

(Xu & Fan, 2022) suggested IDS based on Logarithmic Auto-Encoder (LogAE) and eXtreme Gradient Boosting (XGBoost). The suggested model gave a better performance on the accuracy, meantime, and run time. However, when compare1d to existing IDSs, the run time of the suggested model was not reliable.

(Mittal et al., 2021) introduced the Levenberg-Marquardt Neural network in LEACH protocol (LEACH-LMNN) to reduce energy consumption. The introduced model achieved a high detection rate. Yet, the model was unreliable as the discrimination among the features after the selection was not accurate.

(Zhao et al., 2021) demonstrated an efficient ID method based on Lightweight Dynamic Auto-encoder Network (LDAN). The LDAN extracted strong features, and achieved higher accuracy with reduced computational cost. Yet the model had limation due to high power consumption.

(Zeeshan et al., 2022) deployed a Protocol-Based Deep Intrusion Detection (PB-DID) approach for the Denial of Service (DoS) and Distributed DoS (DDoS) attack detection from IoT traffic. The method had higher accuracy level for ID. However, the model did not concentrate on the mitigation of the attack.

(Gulganwa & Jain, 2022) investigated Energy Efficient and Secure Weighted Clustering Algorithm (EES-WCA) based IDS. The EES-WCA model gave superior results on throughput and end-to-end delay. However, the model was not resistant to zero-day attacks.

(Maheswari & Karthika, 2021) presented a Quality of Service (QoS)-based unequal clustering protocol with IDS in WSNs. The results ensured the better energy efficiency and intrusion detection rate of the presented approach. However, the model was defined for a certain range only.

Proposed Methodology for Energy Efficient Intrusion Detection System in WSN

This paper proposed an energy-efficient intrusion detection system (IDS) in WSNs that aims to mitigate security threats with minimal energy consumption. The architecture of the proposed work is shown in Figure (1).

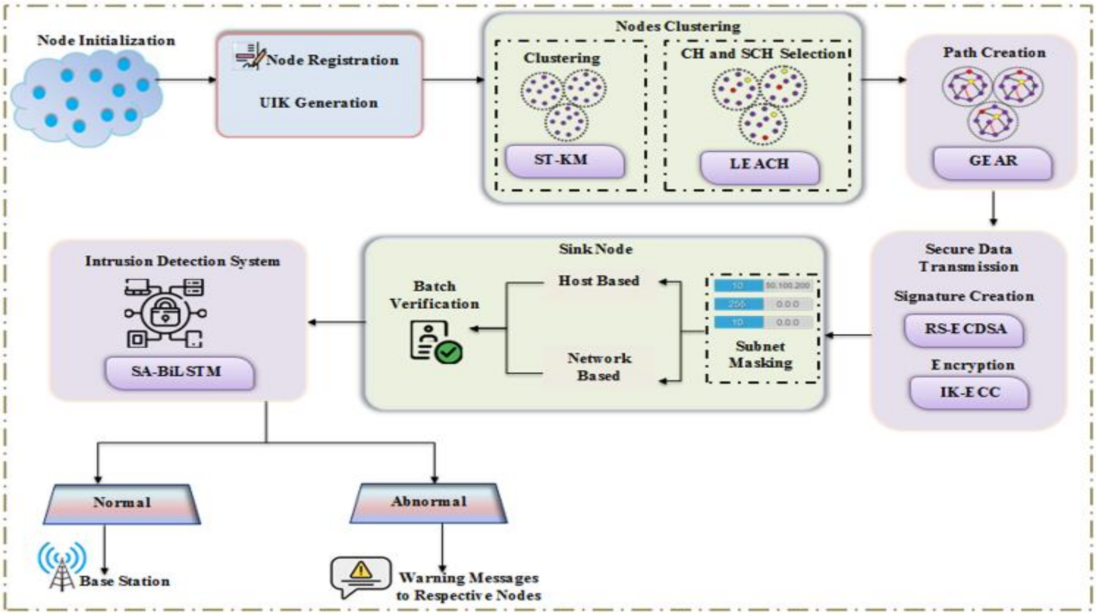

Figure (1): Proposed Framework Architecture.

1. Node Initialization and Registration

Initially, the WS nodes are initialized and registered to the network. The registered nodes (Rn) are mathematically defined by,

$$Rn_k = \{Rn_1, Rn_2, Rn_3, ...Rn_n\} \quad k = 1,2,3,.....,n \quad (1)$$

At the time of registration, each (Rn) is assigned with unique identity key (UIK), which is selected randomly. The generated UIKs (K) are formulated as,

$$K_k = \{K_1, K_2, K_3, ...K_n\} \quad (2)$$

2. Clustering

The, Rn are organized into clusters. The clustering process improves energy efficiency in WSNs. The continuous transmission of data via CH leads to early energy depletion. So, to avoid this, supportive CH (SCH) acts as a backup for CH in case of failure. This extends the overall network lifetime. In this work, clustering is performed by using the ST-KM algorithm. The KM algorithm is computationally efficient and can handle large-scale WSNs with a large number of sensor nodes. However, the KM randomly selects the initial centroids, which causes bias in the clustering results. To avoid this problem, the ST function is used for centroid selection.

Initialize the number of Rn, which is,

$$Rn_k = \{Rn_1, Rn_2, Rn_3, ...Rn_n\} \quad (3)$$

Select the initial centroid (C_k) by ST is given as,

$$C_k = (\lambda - sk) * (\lambda - |\lambda * (Rn_k - \lambda|^W + sk * (\lambda - |\lambda * (Rn_k - \lambda)|^{(1/W)} \quad (4)$$

Where, sk is a parameter that determines the bias of the distribution, W is a parameter that controls the width of the distribution, and $\lambda \in (0,1)$ defines the positive control parameter.

Then, the nodes, which have minimum distance with (C_k), are assigned to the clusters. Thus, the distance $(Dist)$ is,

$$Dist = \sqrt{\sum_{k=1}^{n} (C_k - Rn_k)^2}, \quad (5)$$

Thus, the formed clusters (Cl_i), here (i) defines number of clusters, are expressed by,

$$Cl_i = \{Cl_1, Cl_2, Cl_3, \ldots\ldots, Cl_n\} \quad (6)$$

Pseudo-code for ST-KM is represented below.

Input: Number of registered nodes Rn

Output: Clustering of nodes (Cl_i)

Begin

Initialize the node $Rn_k = \{Rn_1, Rn_2, Rn_3, \ldots\ldots. Rn_n\}$,

Set k value

For $(k = 1 \, to \, n)$ **do**

Compute the initial centroid by using,

$$C_k = (\lambda - sk) * (\lambda - |\lambda * (Rn_k - \lambda|^W + sk * (\lambda - |\lambda * (Rn_k - \lambda)|^{(1/W)}$$

Compute the distance using,

$$Dist = \sqrt{\sum_{k=1}^{n} (C_k - Rn_k)^2},$$

If $Dist == Min$

Assign Rn to the cluster

Else

$k = k + 1$

End if

End for

End

For each cluster, the CH and SCH are selected. The node with maximum residual energy, and minimum distance from other nodes is considered as the CH and SCH. The LEACH protocol is utilized for CH and SCH selection. The key idea of LEACH is to rotate the CH role among nodes to balance the energy consumption across the network. In LEACH, each node generates a random number between 0 and 1, denoted as (X). The node then compares (X) with the threshold (Th). If (X) is less than (Th), then the node becomes CH. The (Th) is calculated as,

$$\boldsymbol{Th} = \frac{\boldsymbol{Pt}}{(1 - \boldsymbol{Pt} * (\boldsymbol{r} \bmod (1/\boldsymbol{Pt})))} \qquad \textbf{(7)}$$

Where, Pt defines the probability at which nodes become CHs in each round r.

3. Path Creation

After clustering, an optimal path is chosen between the nodes within a cluster and their respective CHs and SCHs. Here, in this work, the Geography and Energy Aware Routing (GEAR) protocol is used for path creation.

Generally, the GEAR selects the energy-efficient neighbor as the next-hop node to transmit the data**.** The energy-efficient neighbor is selected based on the estimated cost (E_{cost}) and learning cost (L_{cost}).

The E_{cost} is determined based on the distance between the sender node (node which sends data) (γ) and the CH, and residual energy at the node (γ). The E_{cost} is computed by,

$$\boldsymbol{E_{cost}} = \boldsymbol{wt} \cdot \boldsymbol{\gamma} + (1 - \boldsymbol{wt}) \cdot \boldsymbol{En}(\boldsymbol{\gamma}) \qquad \textbf{(8)}$$

Where, wt refers weight, and $En(\gamma)$ represents consumed energy by (γ).

The L_{cost} typically refers to the computational resources required by individual nodes to transmit the data. The L_{cost} is computed by,

$$L_{cost} = En(\gamma) + E_{cost}(\gamma) + C_t \quad \textbf{(9)}$$

Where, C_t refers to computation cost.

Thus, the node with minimum (E_{cost}) and (L_{cost}) are selected as the next hop node, and performs routing. Thus, the possible routes (Rt) between the source and CHs are created.

4. Secure Data Transmission

Once the routes (Rt) are established, the nodes transmit their data (β_{Data}) to the CH or SCH. To ensure secure transmission, the following processes take place.

(a) Signature Creation

A unique signature is generated using RS-ECDSA for each data packet for recipient verification. ECDSA provides high-level security with relatively shorter key lengths, which results in faster computations and fewer storage requirements. To increase the complexity of the signature, the UIK (K) is incorporated for signature generation.

➢ ***Key Generation***

- First, the elliptic curve is selected; it is defined by the equation

$$A^2 = B^3 + uB + g \quad \textbf{(10)}$$

Where, u, g are the integers, A, B define the function.

- A random integer (G) is chosen as the private key (Pv).
- Then, the public key (Pb) is generated by using,

$$Pb = G * F \quad \textbf{(11)}$$

Where, F defines point on the elliptic curve.

➢ ***Signature Generation***

- The hash value of the message β_{Data} is denoted as HC.
- Then, the random number Rn is generated, i.e. $0<Rn<Y$. Here, Y represents the order of F.
- The signatures Sg_1 and Sg_2 are,

$$Sg_1 = (Pb * K) \bmod Y \tag{12}$$

$$Sg_2 = I(HC + Sg_1 * (Pv * K)) \bmod Y \tag{13}$$

Where, I is the modular multiplicative inverse of Rn modulo Y.

The pair (Sg_1, Sg_2) represents the signature of the hash HC.

(b) Encryption

The data (β_{Data}) is then encrypted using an IK-ECC encryption algorithm to protect its confidentiality during transmission. ECC provides strong cryptographic security but, the exploitation of public parameters of ECC makes it more vulnerable to attacks. To resolve this problem, the UIK is concatenated to the cipher texts.

The (β_{Data}) has the point E on curve Cv. The encryption is performed under two cipher texts CT_1 and CT_2, which are,

$$CT_1 = Rn * E \tag{14}$$

$$CT_2 = [\beta_{Data} + Rn * Pb] + (K) \tag{15}$$

Where, Rn is random number i.e. $0<Rn<Y$, and K is UIK. The encrypted messages are denoted as (Enc_{data}).

5. Sink Node

The (Enc_{data}) are transmitted to the SN, which acts as the gateway to BS. In SN, subnet masking (SM) is performed to distinguish the data from the host side and the network side.

When data arrives at SN, it extracts the source IP address from the data packet. The SN applies SM to both its own IP address and the source IP address. The SM is a binary pattern of 1's and 0's. By performing a bitwise AND operation between the masked IP addresses. If the result of the AND operation matches the SN's IP address, it means the data is from the host side, otherwise from the network side.

6. Batch Verification

At the sink node, batch verification (BV) is carried out. It involves comparing the patterns of (Enc_{data}) with the packets generated by SN itself (S_{pkt}). The SN extracts specific patterns from the (Enc_{data}). Then, the SN generates its own reference packets, which serve as a baseline for comparison. If the pattern of the (Enc_{data}) and (S_{pkt}) is similar, then the (Enc_{data}) is authenticated one; otherwise, transmission is denied. The verified packets are (V_{pkt}).

7. Intrusion Detection System

After the verification, from the (V_{pkt}), the packet details, such as header, payload, source and destination ports, packet size, etc., are inputted to the SA-BiLSTM, which efficiently detects whether the packet is attacked or not.

Bi-LSTM was best but still has vanishing gradient problem. To solve this, the SA function is used. Moreover, the Swish function is non-monotonic, which means it can capture complex interactions and non-linearities in the input. Thereby, more accurate classification can be achieved.

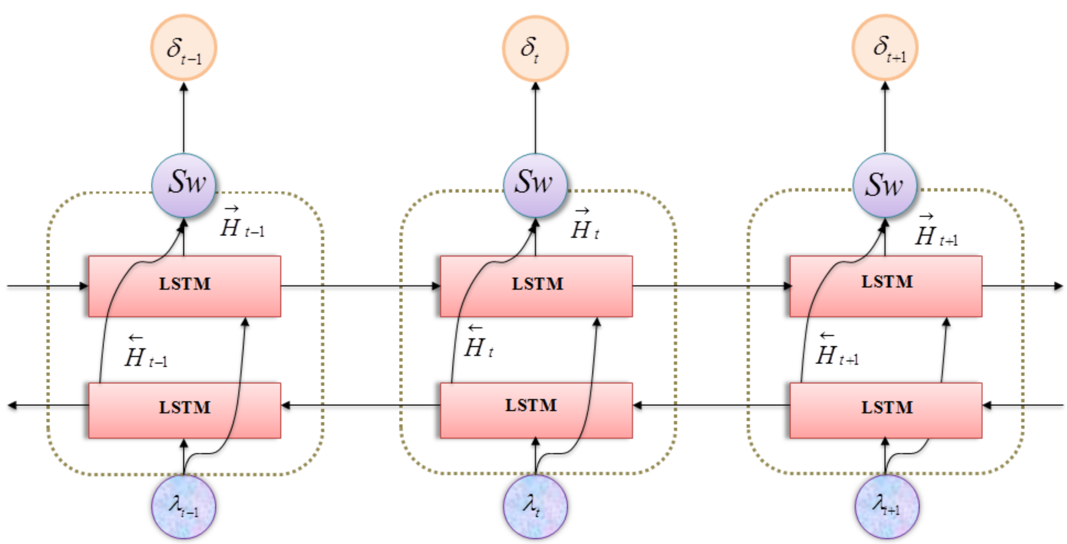

Figure (2): Bi-LSTM Architecture.

Initially, the packet details λ_t are fed into the SA-BiLSTM, which is defined by,

$$\lambda_t = \{\lambda_1, \lambda_2, \lambda_3, ..., \lambda_{t_{Max}}\} \quad \textbf{(16)}$$

Where, t defines time step.

Forward LSTM Computation: The forward LSTM processes the input sequence in a forward direction, from the first to the last time step. At each time step, the following process takes place.

Forget Gate (Fg)**:** It determines which information from the previous cell state (c_{i-1}) should be discarded.

$$Fg_t = Sw[(Wg_{Fg}) \cdot [H_{t-1}, \lambda_t] + Bs_{Fg}] \quad \textbf{(17)}$$

Where, H_{t-1} defines the previous hidden state, Wg_{Fg} and Bs_{Fg} refers to weight and bias of (Fg) respectively, and Sw defines swish activation function, it is given by,

$$Sw(Fg_t) = Fg_t * Sg(\chi * Fg_t) \quad \textbf{(18)}$$

Here, Sg defines sigmoid function, and χ is the controlling parameter.

Input Gate (In_t)**:** It determines which new information should be added to the current cell state.

$$In_t = Sw(Wg_{In}) \cdot [H_{t-1}, \lambda_t] + Bs_{In} \quad \textbf{(19)}$$

Where, Wg_{In} and Bs_{In} refers to weight and bias of (In_t) respectively.

Output Gate (Ot_t)**:** The outcome from the (H_t) is fed into the (Ot_t).

$$Ot_t = Sw(Wg_{Ot}) \cdot [H_{t-1}, \lambda_t] + Bs_{Ot} \quad \textbf{(20)}$$

Where, Wg_{Ot} and Bs_{Ot} refers to weight and bias of (Ot_t) respectively.

Backward LSTM Computation: The backward LSTM processes the input sequence in a backward direction, here, the reverse process as in the forward LSTM is performed.

Output Computation: The output (δ_t) is obtained by combining the forward $(\overrightarrow{H_t})$ and backward hidden states $(\overleftarrow{H_t})$ at each time step.

$$\delta_t = [H_t + H_t] \qquad (21)$$

Then, (δ_t) detects whether the data packets are normal or abnormal. If it is normal, the packets are transmitted. Otherwise, the transmission gets declined and sends warning messages to the corresponding node. Thus, the proposed method ensures the integrity of data in the WSN with a lower energy rate.

Results and Discussions

The performance evaluation of the proposed work is carried out in this section. The implementation is done in PYTHON.

1 Dataset Description

UNSW-NB15 dataset consists of approximately 2.5 million instances, making it a relatively large dataset for network intrusion detection. It was generated by researchers at the University of New South Wales (UNSW) in Australia. 175341 data were utilized for the training and 82332 data were used for testing the proposed model.

2 Performance Analysis

In this section, the performance of the proposed method is validated.

Table (1): Energy Efficiency Analysis.

Techniques	Energy consumption (J)
Proposed ST-KM	11143
KM	12654
K-medoid	13153
FCM	13897
CLARA	14479

Table (1) provides the energy consumption rate of the proposed ST-KM and the existing KM, K-medoid, Fuzzy C-Means (FCM), and Clustering large application (CLARA). The proposed clustering technique uses CH and SCH for data transmission. Thus, the proposed ST-KM consumes 11143 J of energy. Thus, the proposed model is energy efficient.

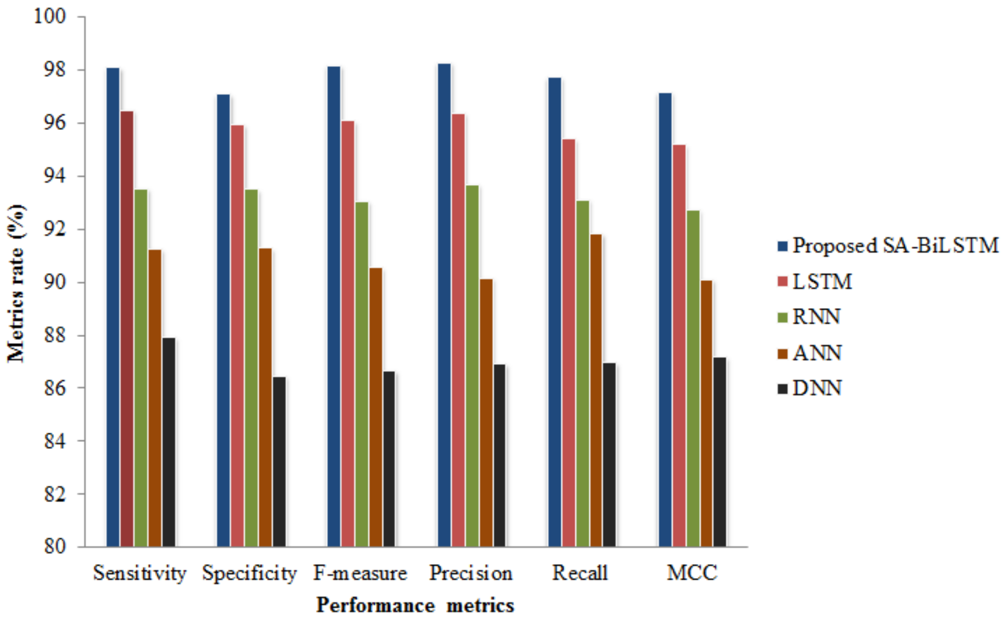

Figure (3): Performance Comparison.

Figure (3) compares the performance of the proposed SA-BiLSTM with existing methods, such as LSTM, Recurrent neural network (RNN), Artificial NN (ANN), and Deep NN (DNN). The proposed SA-BiLSTM uses the SA function, which keeps the neurons, remains active for a long time. So, the proposed SA-BiLSTM achieves a 98.26% of detection rate, 98.13% of sensitivity, 97.12% of specificity, 98.2% of F-measure, 98.31% of precision, and 97.75% of recall, whereas the existing techniques obtain lower performance rates. Thus, the proposed SA-BiLSTM classifies normal and abnormal data efficiently.

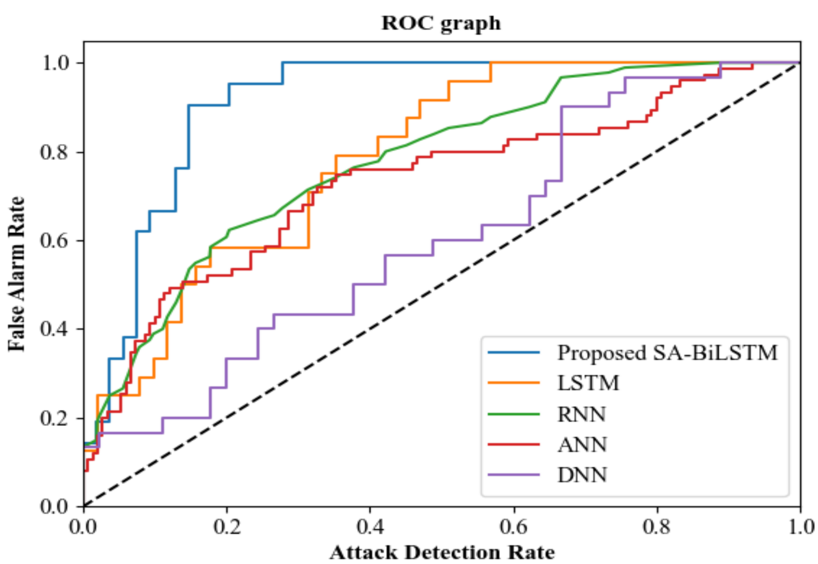

Figure (4): Comparison of ADR and FAR.

Figure (4) compares the Attack Detection Rate (ADR) and FAR of the proposed SA-BiLSTM and the existing techniques. From the figure, it is clear that the proposed SA-BiLSTM detects the attacks at the rate of 98.89% with a FAR of 2.11%. This is because the SA-BiLSTM uses SA function, which improves the flow of gradients through the network and improves the learning process.

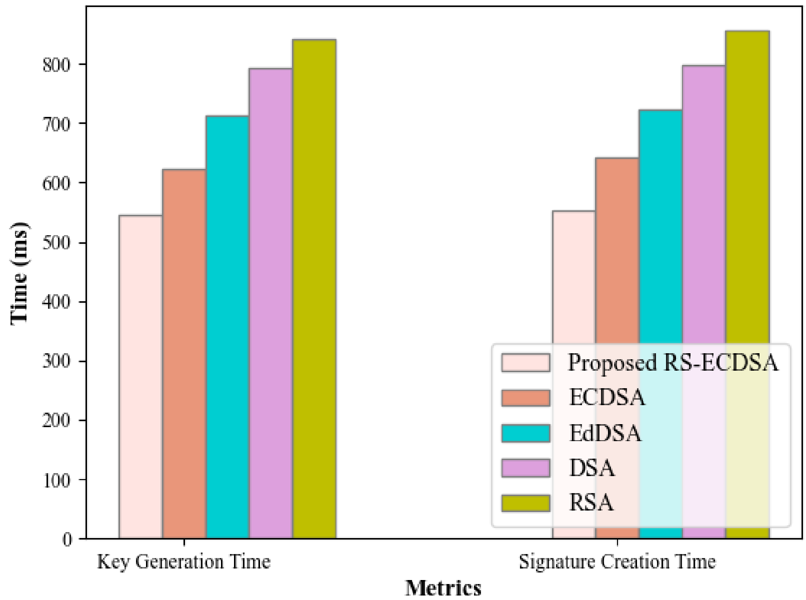

Figure (5): Comparison of Key Generation and Signature Creation Time.

Figure (5) shows the performance of the proposed RS-ECDSA and the existing ECDSA, Edward curve DSA, DSA, and Rivest-Shamir-Adleman (RSA). The proposed method creates the keys and signatures at the time of 545 ms and 552 ms, respectively. This is because RS-ECDSA has faster computation properties. Thus, the time complexity of the proposed work is very low.

Table (2): Performance Evaluation of the Proposed IK-ECC.

Techniques	**Performance metrics**		
	Encryption time (ms)	**Memory usage (kb)**	**Security level (%)**
Proposed IK-ECC	1087	4364066	98
ECC	1176	4967184	96
Diffie-Hellman	1212	5473821	93
ElGamal	1298	5926408	90
RSA	1325	6315965	86

Table (2) depicts the performance of the proposed IK-ECC and the existing works. In the proposed IK-ECC, more secure keys with shorter sizes are used. So, the proposed IK-ECC requires 1087 ms to encrypt the data with a memory usage of 4364066 kb and withstands with better security of 98%. This is comparatively higher than the existing techniques.

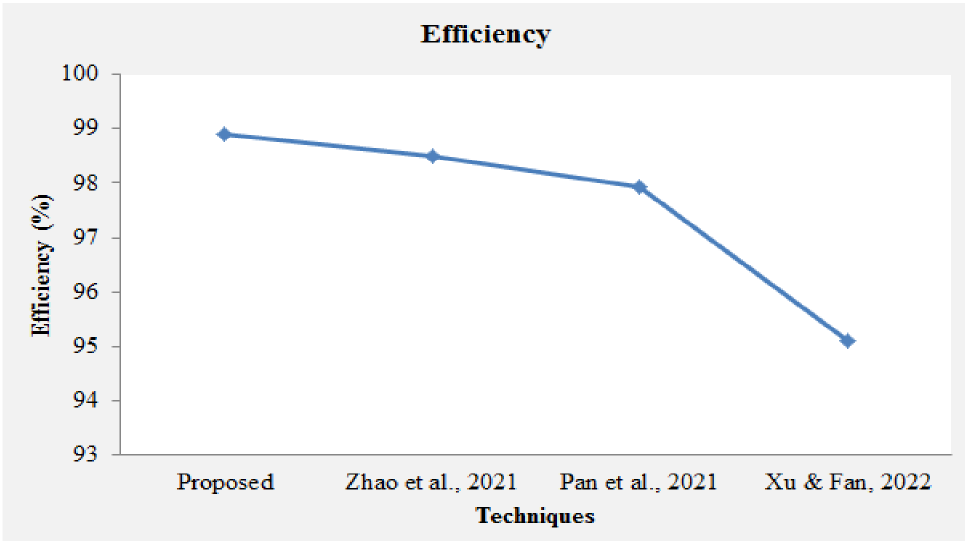

Figure (6): Efficiency Comparison with Prevailing Methods.

Figure (6) compares the efficiency of the proposed methodology with the existing research methodologies. The proposed method provides an additional layer of security by increasing the complexity of the signature and encryption process. It helps to prevent attackers from easily accessing the transaction data. From the analysis, it is clearly understood that the proposed method withstands better efficiency as compared to existing works.

Table (3): Parameters of the Classifier.

Parameters	Proposed SA-BiLSTM	LSTM	RNN	ANN	DNN
Activation function	Smish	tanh	ReLu	ReLu	Relu
Optimizer	Adam	Adam	Adam	Adam	Adam
learning rate	0.01	0.001	0.001	0.001	0.001
Batch size	32	32	784	128	128
Epochs	100	100	100	100	100
Execution time	12315	15324	16731	17211	17934

Table (3) depicts the training parameters of the proposed SA-BiLSTM model and the traditional LSTM, RNN, ANN, and DNN models. Here, the improved learning rate and the least execution time of the proposed SA-BiLSTM prove that smish activation performs well for the detection of intrusion in the network.

Conclusion

This work has proposed an energy-efficient intrusion detection system in WSN using IK-ECC and SA-BiLSTM. The approach includes several operations, such as node registration, UIK generation, clustering, CH and SCH selection, path creation, signature creation, encryption, subnet masking, batch verification, and ID. After that, the experimentation analysis is performed in which the performance and the comparative analysis of the proposed techniques are carried out to validate the effectiveness of the work. The developed approach can handle various uncertainties and renders more promising results. The UNSW-NB15 dataset is used for the analysis in which the proposed method achieves 98.89% of ADR. Overall, the proposed framework outperforms the existing state-of-art methods and remains to be more reliable and robust. However, this work concentrated on the energy-efficient IDS based on cryptographic techniques, which have centralized control. Thus, in the future, the work can be enhanced by using decentralized control for node authentication and authorization.

References

- Ahmad, Z., Shahid Khan, A., Wai Shiang, C., Abdullah, J., & Ahmad, F. (2021). Network intrusion detection system: A systematic study of machine learning and deep learning approaches. Transactions on Emerging Telecommunications Technologies, 32(1), 1–29. https://doi.org/10.1002/ett.4150.

- Basha, A. R. (2020). Energy efficient aggregation technique-based realisable secure aware routing protocol for wireless sensor network. IET Wireless Sensor Systems, 10(4), 166–174. https://doi.org/10.1049/iet-wss.2019.017.

- Dwivedi, S., Vardhan, M., & Tripathi, S. (2021). Building an efficient intrusion detection system using grasshopper optimization algorithm for anomaly detection. Cluster Computing, 24(3), 1881–1900. https://doi.org/10.1007/s10586-020-03229-5.

- Fang, W., Zhang, W., Yang, W., Li, Z., Gao, W., & Yang, Y. (2021). Trust management-based and energy efficient hierarchical routing protocol in wireless sensor networks. Digital Communications and Networks, 7(4), 470–478. https://doi.org/10.1016/j.dcan.2021.03.005.

- Gulganwa, P., & Jain, S. (2022). EES-WCA: energy efficient and secure weighted clustering for WSN using machine learning approach. International Journal of

Information Technology, 14(1), 135–144. https://doi.org/10.1007/s41870-021-00744-5.

- Hammad, M., El-Medany, W., & Ismail, Y. (2020). Intrusion detection system using feature selection with clustering and classification machine learning algorithms on the UNSW-NB15 dataset. 2020 International Conference on Innovation and Intelligence for Informatics, Computing and Technologies, 52, 3–8. https://doi.org/10.1109/3ICT51146.2020.9312002.

- Kasongo, S. M., & Sun, Y. (2020). Performance analysis of intrusion detection systems using a feature selection method on the UNSW-NB15 dataset. Journal of Big Data, 7(1), 1-20. https://doi.org/10.1186/s40537-020-00379-6.

- Maheswari, M., & Karthika, R. A. (2021). A novel QoS based secure unequal clustering protocol with intrusion detection system in wireless sensor networks. Wireless Personal Communications, 118(2), 1535–1557. https://doi.org/10.1007/s11277-021-08101-2.

- Mittal, M., Iwendi, C., Khan, S., & Rehman Javed, A. (2021). Analysis of security and energy efficiency for shortest route discovery in low-energy adaptive clustering hierarchy protocol using Levenberg-Marquardt neural network and gated recurrent unit for intrusion detection system. Transactions on Emerging Telecommunications Technologies, 32(6), 1–16. https://doi.org/10.1002/ett.3997.

- Pan, J. S., Fan, F., Chu, S. C., Zhao, H. Q., & Liu, G. Y. (2021). A lightweight intelligent intrusion detection model for wireless sensor networks. Security and Communication Networks, 2021, 1-15. https://doi.org/10.1155/2021/5540895.

- Prithi, S., & Sumathi, S. (2020). LD2FA-PSO: A novel learning dynamic deterministic finite automata with PSO algorithm for secured energy efficient routing in wireless sensor network. Ad Hoc Networks, 97, 102024. https://doi.org/10.1016/j.adhoc.2019.102024.

- Prithi, S., & Sumathi, S. (2021). Automata Based Hybrid PSO–GWO Algorithm for Secured Energy Efficient Optimal Routing in Wireless Sensor Network. Wireless Personal Communications, 117(2), 545–559. https://doi.org/10.1007/s11277-020-07882-2.

- Raiyat Aliabadi, M., Seltzer, M., Vahidi Asl, M., & Ghavamizadeh, R. (2021). ARTINALI#: An efficient intrusion detection technique for resource-constrained cyber-physical systems. International Journal of Critical Infrastructure Protection, 33, 100430. https://doi.org/10.1016/j.ijcip.2021.100430.

- Ramadan, R. A. (2020). Efficient intrusion detection algorithms for smart cities-based wireless sensing technologies. Journal of Sensor and Actuator Networks, 9(3), 1–22. https://doi.org/10.3390/JSAN9030039.

- Xu, W., & Fan, Y. (2022). Intrusion detection systems based on logarithmic autoencoder and XGBoost. Security and Communication Networks, 2022,1-8. https://doi.org/10.1155/2022/9068724.

- Zeeshan, M., Riaz, Q., Bilal, M. A., Shahzad, M. K., Jabeen, H., Haider, S. A., & Rahim, A. (2022). Protocol-based deep intrusion detection for DoS and DDoS attacks using UNSW-NB15 and Bot-IoT data-sets. IEEE Access, 10, 2269–2283. https://doi.org/10.1109/ACCESS.2021.3137201.

- Zhao, R., Yin, J., Xue, Z., Gui, G., Adebisi, B., Ohtsuki, T., Gacanin, H., & Sari, H. (2021). An efficient intrusion detection method based on dynamic autoencoder. IEEE Wireless Communications Letters, 10(8), 1707–1711. https://doi.org/10.1109/LWC.2021.3077946.