EAI Endorsed Transactions
on Internet of Things
Review Article EAI.EU

Comparative Study on Anomaly based Intrusion Detection using Deep Learning Techniques

Sabeena S[1,*], Chitra S[2]

[1,2]Department of Computer Science, Bishop Heber College, Bharathidasan University, Trichy, India

Abstract

With an array of applications, Wireless Sensor Networks (WSNs) have the potential to transform the world into a smart planet. WSNs consist of a collection of resource-constrained sensors that gather data, which is then utilized for decision-making and analysis, leading to improvements in quality of service, management, and efficiency. However, the open nature of WSNs exposes them to numerous vulnerabilities and threats. Operating in potentially hostile and unattended environments makes these networks attractive targets for adversaries. Therefore, it is essential to detect the presence of malicious attacks within the networks and implement robust security systems to address these challenges. While traditional security mechanisms such as authentication and cryptographic methods are commonly employed, they often fall short in effectively countering the dynamic nature of modern attacks. Hence, IDS (Intrusion Detection System) tends to continuously monitor the network and detect potential threats in real-time scenarios. This method possess the ability of identifying, responding promptly, preventing and thus ensures resilience of the network. Therefore, the present study reviews the various intrusion detection techniques and data collection methods. The main aim of the study is to investigate the design challenges of deploying IDS in a WSN environment. So, the study analysed the AI (Artificial Intelligence) based techniques involved in intrusion detection and how these techniques could be adopted in WSN. In addition, the comparative analysis of several ML (Machine Learning) and DL (Deep Learning) algorithms are also deliberated to portray the different deployment technique with corresponding outcomes. Further, the main challenges faced by each studies with their limitations are specified for supporting future researchers in developing new trends in intrusion detection for WSN.

Keywords: Wireless Sensor Network, Malicious Attacks, Intrusion Detection Systems, Machine Learning, Deep Learning

Received on 03 09 2024, accepted on 17 11 2024, published on 27 11 2024

doi: 10.4108/eetiot.7178

1. Introduction

In recent times, the WSN are becoming significant in various sectors such as medicine, environment, transportation and industrial sectors. Additionally, the advancements in the wireless communication, computer network, signal processing, microcomputer electrical system and microelectronics has emerged the intelligent characteristics of WSN [1, 2]. Some wide applications of WSN includes the no gateways, dynamically changeable routing, resource constrained sensor nodes, monitoring distribution and small size. With the vast developments of WSN, the increase in the intrusion of attacks has also

*Corresponding author. Email: sabeenashameem1990@gmail.com

emerged as the major concern. So, various researches are focusing on detection of attacks in the network, encryption methods and key managements along with effective network security architectures. Generally, WSN is defined as the interlinked multifunctional devices such as sensors called as nodes. These nodes are placed in the area of interest with atleast one sink node known as BS (Base Station), which provides communication with network end users and applies centralised control over the network. Specifically, the sensor node comprises of a power unit, sensing elements, communication module and a processing unit [3]. Moreover, the network may also consist of positional tracking or mobility module. In WSN, the power unit is the battery, whereas the sensor nodes uses the sensing components to collect the data and then uses processing unit to handle the collected data. On the other hand, the communication module is utilised to wirelessly exchange the data with BS and other sensor nodes. Further, the position tracking unit verifies the present location of the sensor nodes and the mobility module produces transportability. The most significant concern in security of WSN is the intrusion of malware attacks [4]. The evolution of attacks created a great challenge in the designing IDS, to identify and prevent the entry of attacks into the network. Several studies have concentrated in investigating the conventional algorithms, data mining and the nature inspired communicational protocols. But these methods tend to provide large amount of computational overhead, which severely limits the real-time deployment and practical applications of WSN. Only few studies focussed in deliberating the AI [2] based IDS in WSN, which increases the detection accuracy and reduced computational overhead of IDS. So, the current study engaged in reviewing the existing studies involved in the intrusion detection of malware in WSN by comparing the various communication protocols.

In contrary, several approaches applied artificial immune principles such as dendritic cell method, danger theory and negative selection techniques in IDS of WSN. So, the considered study [5] implements the negative selection method based on spatial partition and is used in the hierarchical WSN. Initially, the algorithm analyses the distribution of self-set in the real-valued space and then categorises the real-valued space, where various subspaces are produced. Then the negative selection technique is applied in the subspace, in which the tolerance range of candidate detector and thus protects the resources of sensor nodes. Further, in the process of predicting the detectors, the antigen should correlate with the matured detectors in the subspace. This accelerates the antigen detection process and thus decreases the time cost of distance calculation. Similarly, the ensemble learning approach, based on the Bagging algorithm and information gain ratio is employed in the intrusion detection model for WSN [6]. At first, the information gain ratio is utilised to choose the sensor node traffic data feature and then the bagging algorithm is used to develop an ensemble classifier. This is utilised to train several C4.5 DTs (Decision Trees) and the parameter optimisation of ensemble classifier is performed by applying 10 iterations. Finally, the outcomes of C4.5 DT are classified and by majority voting approach, the intrusion is detected. From analysis, it is found that the model produced enhanced detection accuracy of scheduling, flooding, Gray-hole, Blackhole and other types of intrusion attacks. In the case of predicting the attacks that causes damage to WSN system within a short duration of time, the suggested study analyses the intrusion of such attacks. So, the study [7] implements the fusion of SBS (Sequence Backward Selection) and LGBM (Light Gradient Boosting Method) to predict the intrusion in WSN. The SBS algorithm is deployed in order to shrink the data dimension on feature space of original traffic data, which in turn reduces the computational overhead and communication burden. The SBS decrease the probability of information loss and thus enhances the detection accuracy of LGBM classifier. In this way, the LGBM uses two improved algorithms such as EFB (Exclusive Feature Bundling) and GOSS (Gradient based One Side Sampling). By using GOSS algorithm, the number of samples per round of training is decreased and the features are reduced by using EFB technique. The outcomes of the study projects that the detection rate is increased with reduced false alarm rate.

In the last few years, the advancements of AI techniques such as ML and DL algorithms increased the opportunities to mitigate the challenges faced by the IDS. So, the present study focusses in reviewing the up to date taxonomy of significant researches implemented in the detection of intrusion in WSN. It provides the comprehensive and structured overview of existing IDS in WSN, so that the researchers are capable of analysing and gain a quick knowledge on the key aspects to build an effective AI based IDS in WSN. The study reviewed the detection approaches, validation strategies, deployment techniques used in various studies. Further, the complexity and evaluation techniques deployed in various detection algorithms are critically reviewed. Followed by a set of suggestions regarding the optimised techniques are discussed to effectively analyse the better enhanced methods used in the detection of IDS in WSN. Previous studies have not completely conferred the wide ranging study of IDS, so the present study concentrated on reviewing the datasets, techniques, limitations and challenges.

The main contributions of the study are as follows,

- To study the detection approaches employed in IDS in WSN based on AI techniques, to effectively address the limitations of IDS in other conventional methods.
- To analyse the limitations and challenges of the algorithms used in IDS, which helps future researchers to identify the key aspects to overcome the mitigation.
- To exhibit comparative analysis of various AI based approaches in IDS of WSN, to easily predict effective methods involved in intrusion detection and classification of malwares in WSN.

1.1 Paper Organisation

The present study reviews the techniques involved in the intrusion detection in WSN, which started with the introduction section, along with survey methodology deliberated in Section 2; the overview of WSN and the corresponding security attacks are conferred in Sections 3. Then the significance if IDS in WSN is explained in Section 4. Further, the different algorithms based on AI techniques is discussed in Section 5. The comparative analysis of various ML and DL based techniques are represented in Section 6. Further, the research gaps with the future scope of the study is signified in Section 7. Finally, the paper is concluded in Section 8.

2. Survey Methodology

The survey methodology is developed by assessing studies from “Google Scholar”. The conventional studies relevant to the concept of present study are searched by using keywords "Security Threats in Wireless Sensor Networks," "Intrusion Detection Systems", "AI based IDS in WSN," and "ML based IDS", “Intrusion Detection using DL Algorithms”. The suitable and correlated publications were selected from papers published between 2019 and 2023. Initially, the title-related to the papers were selected and then the screening process of studies were held based on abstract. If relevant, the overall text was also considered. Additionally, citations of the paper were added sufficient to critically analyse the review, with total refined studies of 40 corresponding to the concept. Figure. 1 represents the survey methodology considering four different processes used in the study.

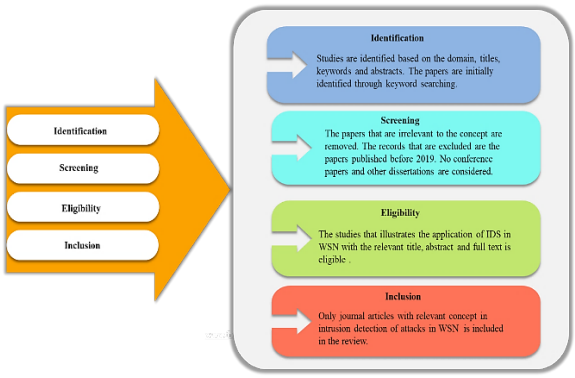

Figure 1. Survey Methodology

3. Gestalt of Wireless Sensor Networks and Security Attacks 1

The WSN is a collection of wireless sensor nodes deployed in the unstructured circumstances, in which it gathers the data and then process according to assigned tasks. These techniques are widely used in several applications, and is extended from general to specific purposes. Based on the size variation, transmitting and receiving abilities, and processing time, the cost of the wireless nodes varies [8]. The structure of WSN depends on the deployment environment and is mainly divided into three types namely hierarchical, flat and cluster based networks. Moreover, the sensor devices placed in remote, harsh and inaccessible locations tends to provide reduced communication, bandwidth, power and storage. This denotes the sensor nodes plays a significant part in the WSN to transfer data from one node to the other pre-defined nodes under broaden range. Similar to WSN, the wireless adhoc networks can also generate automatic sensor structure that is able to transmit data in wireless form [9]. The figure.2, represents the systematic illustration of WSN.

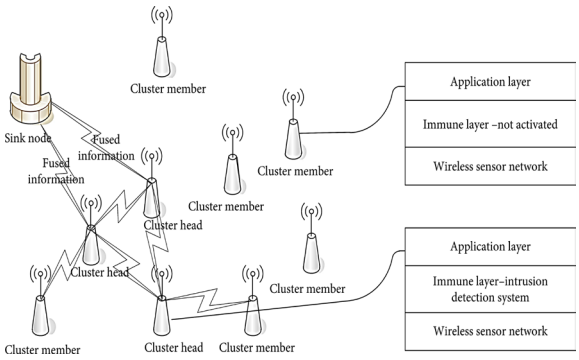

Figure 2. Systematic Illustration of Wireless Sensor Network [5]

The major difference among the WSN and wireless adhoc networks are as follows,

- More sensor nodes are required in wireless adhoc network, while WSN comprises of limited sensor nodes.
- The wireless adhoc network consisting of sensor nodes, should be employed in a densely connected form. If not placed in appropriate place, then the sensor nodes are confronted with redundancy.
- Failure occurs in the sensor nodes when the obtaining power connection from other nodes. These nodes also possess restrictions with memory, computational efficiency and power.

Based on the limitations of wireless adhoc networks, the WSN ensures better advantages in terms of accuracy, cost and power. Generally, the sensor nodes works under the use of non-rechargeable battery lasting over several months or years, but consumes energy while transmitting and receiving the data. Here, the energy efficiency is the major concern and is used in enhancing the life expectancy of the network. So, appropriate selection of cluster heads is an important key aspect, through which the communication link is provided between the sink and WSN. In case of clustered communication, the sensor nodes of the wireless network are accumulated into small sets known as cluster [10]. The cluster comprises of a cluster head, which associates the data grouping and aggregation method in a specific cluster. Moreover, the data packets are transmitted to the cluster head through any node of that cluster. As the clustering technique improves local decisions and need for central organisation, the scalability of WSN is thus enhanced.

In clustering, the transmission of data is performed under two steps through intra-cluster and inter-cluster. First, in the intra-cluster method, the data is transferred between the cluster head and cluster member sensor nodes. Whereas, in inter-cluster method, the data is transmitted among the BS and cluster head. However, the inter-cluster data transfer in WSN can be either single hop or multi-hop communication. Basically, the single hop is used only when the distance between the BS and cluster head is less or small when compared with the threshold distance. On the other hand, the multi-hop communication is applicable only when the distance among the BS and cluster head is large. So, to optimise the life-time and scalability of WSN, the multi-hop communication is chosen than single hop communication protocol [11]. Nevertheless, some sensor nodes may not get combined during the cluster formation or they may have been placed far of distance from the cluster head. Hence, a sub-clustering is employed to mitigate the issue by covering all the far way nodes. This is done as these sensor nodes may possess some important information.

3.1 Security Attacks

The open nature of wireless data transmission throws some severe problems like reliability, security and privacy. As wireless networks process and transmits various sensitive data, corresponding data security concerns are necessary to tackle the intrusion of adversaries. By the entry of adversaries, the sensors are seized, re-programmed and make it to transfer fabricated data readings causing endangered lives and disastrous consequences [12]. Thus, due to lack of security providence, the energy of sensors are depleted as they are continuously indulged in sensing and transferring false data readings prominent to disabled network system. So, in order to provide efficient security to the network, the intrusion of attacks has to be detected to make the system reliable. Moreover, many-to-one communication system in WSN causes additional vulnerabilities to the network, since all nodes transmit data to the BS. So, WSN is wide-open to two different types of attack namely insider and outsider attacks. The insider attacks generally arises only when the aggressor breaches a sensor node and use that node to activate another attack or launch an attack on the same domain. Wherein, the outsider attack ascends when the aggressor intrudes the external entity to corrupt the functionality the network. The main insider attack is the blackhole or sinkhole attack that is specifically denoted as the active routing disruption attack applied on the network layer. Here, the attacker node grasps the attention of other nodes by publicizing itself as a high quality routing path to BS. Thus, the nodes frequently utilises the malicious node path that alters the transmitted data packets making the BS unable to receive the complete and correct data. The major security objectives in WSN are as follows [13],

1. **Data confidentiality:** One of the main objective of security concern in WSN is the data confidentiality, which refers to the service of providing guarantee to the data. In this aspect, the data is made assessable only to the entities. Generally, the standard method to secure the sensitive data is by employing encryption using public key. But these approaches are expensive to be applied in the sensor networks. So, several security protocols in WSN uses systematic cryptosystem based cryptographic methods.

2. **Availability:** Availability signifies the system properties permitting the authorised entity to access within the indicated limit.

In WSN, the availability remains complex and the node does not provide information to protect the computational capability, memory and energy supply.

3. **Location Security:** A malicious node tend to extract the information location to destabilise the operations of the network. So, the location is considered as the significant factor for efficient functioning of the network. However, the sensor network should possess the ability of automatically locating every sensor present in the network. Thus, it is essential to monitor the location security to provide optimised security network.

4. **Data Freshness:** The main objective of data freshness is that only recent data is concerned and no old information of messages are retransmitted by the attacker. In order to tackle the problem, the old information are filtered by adding a sequence number to data packets.
5. **Authentication:** The authentication represents the identity verification of nodes and if authentication is managed poorly, then the attacker can easily access the network. If the communication with right node is not assured then the integrity and confidentiality of the exchanged information cannot be assured. As the wireless medium is employed in the unattended and hostile areas, it is complex to ensure authentication of data.

6. **Integrity:** If the data is transmitted through the network accidentally or voluntarily, then integrity assures that the data not being altered. Thus, data integrity targets in preventing the data against accidental changes of legal arbitrates.

Though there are several existing studies focussed on the security mechanism in WSN such as private and public key cryptographic methods, they cannot be adopted in WSN [14]. This is due to the demand on higher computational adequacy producing decreased lifetime and efficiency of the network. Other traditional approaches operates based on defining a trustworthiness threshold and on the mobile agents. These methods suffer for incapability to predict more than one attacker node or tampering data at a specific time period. Therefore, security techniques that do not affect the effectiveness of the network should be deployed.

4. Significance of Intrusion Detection in Wireless Sensor Networks

In today's big data era, WSN technology has been continuously developing with the increase in intrusions. Generally, the traditional intrusion detection methods includes artificial immune detection and other information theory. These methods possess some shortcomings and with the increase in complications the model tend to generate issues related with low detection rate, poor attentiveness and high false alarm rate [15]. Hence, it is crucial to develop an IDS in order to enhance the security defence capabilities of WSN. Moreover, to enhance the proactive defence capabilities of the model, it is significant to improve the detection accuracy level to achieve the development of IDS with good scalability and self-adaptability [16]. Thus, the profound usage of internet has increasingly urged researches on anti-intrusion and intrusion. The development level of anti-intrusion technique lags creating a larger dilemma and thus it is extremely required to innovate and optimise the IDS. The figure.3 shows the intrusion detection in WSN.

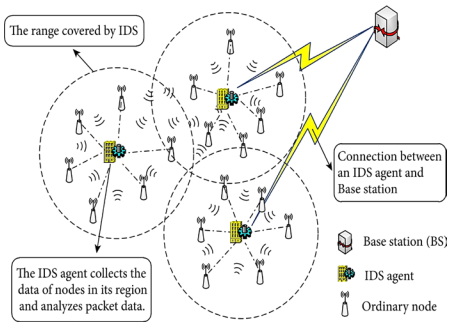

Figure 3. Intrusion Detection Model applied in Wireless Sensor Network [17]

The cryptography, firewalls and other network security techniques have not been developed to overcome the threats such as Trojans, viruses, worms, DoS and DDoS attacks. The intrusions are detected by continuous monitoring of misuse in IDS regarding the vulnerability signatures [18]. Cyber-attacks on large data are emerging in recent days, since the conventional methods have lacked in detecting the attacks. Major studies lacks in predicting the unknown threats and do not provide real time solutions to overcome the hurdles. In the intention of identifying the abnormalities, there are several number of detection methods and are categorised into statistical methods, data mining techniques, ML and DL algorithms.

5. Artificial Intelligence based Intrusion Detection Systems

A variety of assaults are being regularly attempted in different network infrastructures due to the growth of internet usage globally. The traditional intrusion detection methods are not sufficient for huge data. One most significant solution for rectifying the issues related with intrusion detection is the use of AI that recognises complex patterns in the input data samples to predict the anomalies [19, 20]. Thus, the need for effective techniques can be mitigated by using AI algorithms such as ML and DL methods. This section provides the different methods involved in intrusion detection for WSN with corresponding strengths and limitations.

5.1. Intrusion Detection System using Machine Learning

The ML techniques can enhance the efficiency of intrusion detection in WSN. The ML algorithms [21] are classified into three different type's namely supervised, semi-supervised and unsupervised methods. In context of supervised algorithm, the labelled input is fed into the model for training purposes. And based on the label, the different classes are categorised according to the dataset. Whereas, the semi-supervised method deploys a few labelled data with several unlabelled data. Thus, the precision of the semi-supervised algorithm can be enhanced by applying both unlabelled and labelled data. In the unsupervised technique, the unlabelled input data is passed into the system and thus figures out the structure of correlation in the input. So, with the use of ML technique, the intrusion detection can be applied effectively.

Contemporarily, the ML methods uses algorithms and statistics to detect the intrusion in the network. Hence, the considered study [22] has implemented ML algorithms based on BFS-GSRF (Boruta Feature Selection with Grid Search Random Forest) to overcome the misclassification of intrusions and poor accuracy production. The study has involved pre-processing method, feature selection technique and then classification. After pre-processing, the features has been selected by using wrapper approach, which measures the usability of features. The feature extraction has been performed by Boruta algorithm that helps in selecting features when several features are present in the dataset. This method has eradicated the redundant variables and thus predicts the significant variables. The BFS-GSRF algorithms has been derived by adding the randomness to the system, thus accumulating the outcomes from the ensemble of randomised set. In order to perform classification of data, the RFGS has been utilised, where different classification trees for identifying the target class. Depending on the majority votes, the final detection has been done and thus parameter optimisation has enhanced the accuracy of the system. Here, the main purpose of optimisation has to decrease the OOB (Out of Bag) error. From analysis, the study has produced better outcomes in terms of accuracy. However, the Boruta has been prone to infinite loop, by which this method is not good enough to generate increased precision with superior multi-classification. This has also been restricted based on time and this can be mitigated by employing higher-level programming platforms. Similarly, the suggested study [23] has employed the ML algorithm known as ensemble learning to enhance the detection of intrusion in the dataset. The study has focussed in two types of classification techniques such as single classifiers and the ensembles. The single classifiers includes the SVM (Support Vector Machine), K-NN (K-Nearest Neighbour), NB (Naïve Bayes), PA (Passive Aggressive), P (Perceptron), HT (Hoeffding Tree) and HAT (Hoeffding Adaptive Tree). On the other hand, the ensembles involves the heterogeneous and homogenous ensembles. An online ensemble approach has been deployed to provide higher detection rate in classifying the malicious attacks. The study has analysed different online ensemble classifiers to predict the best classifier and based on the outcomes, NB, ARF and HAT algorithms has been selected as the base learners for heterogeneous ensembles. Further, a majority vote ensemble has been utilised to integrate the outcomes of two stable learners to incur improved precision and speed at the same time. Thus, the results produced by the study has found to be enhanced in detection of malicious attacks. But the study has not concentrated in improving the parameter tuning and data reduction through pre-processing technique. Thus leading to reduced efficiency of the classifier.

The network defenders should be cautious in monitoring the cyber threats. So, the intimated study [24] has deployed a feature extraction method based on CFS (Correlation Based Feature Extraction), to reduce the computational time and increase the efficiency of the system. In this study, the main objective of CFS has to assess the redundancy and relevance of particular feature subset that has been searched in the specified search space for ideal solution. The features has been chosen based on the correlation based assessment function, which selects the subsets with extraordinarily correlating with the class and uncorrelating with each other. Here, a trust value of a node has been evaluated based on the residual energy level and behavioural analysis of nodes. The study has used SRFA (Secured RF Algorithm), which is the combination of CART (Regression Tree) along with Bagging method and unpruned classifiers. Based on the selected features, the SRFA algorithms has selected the best feature

and thus has developed the DT. From analysis, it has been predicted that the study has produced better accuracy results in both small and large datasets. Furthermore, the considered study [25] has applied SMOTE (Synthetic Minority Oversampling Technique), in order to tackle the class imbalance of intrusion dataset. The SMOTE has inserted new randomly produced samples, which has enhanced the number of minority class samples. It has also oversampled the dataset, where the training set has been reconstructed and the original class samples has been balanced. Then the RF classifier has been utilised to train the samples and to realise the intrusion detection for WSN. This classifier has tend to overcome the over-fitting issues of DT and has possessed better scalability and tolerance to anomaly and noise values. Here, the comparison of the algorithms has been performed with Adaboost M1, Bagging, NB, LiBSVM and J48 techniques. Before combining RF with SMOTE, the system has produced 92.39% accuracy and after combining 92.57% accuracy has been produced by the study. Thus, this study has provided effective way to resolve the issues of imbalance dataset and thus has increased the accuracy of intrusion detection in WSN. However, the study has to improve the recognition rate of intrusion data to provide effective prediction of attacks in the given dataset.

Alternatively, warfare and political aspects of attacks on critical and industrial infrastructure are emerging to be more relevant. An efficient intrusion detection systems is essential as threats on industry with the legal requirements are becoming prevalent. Hence, the intimated study [26] has employed ML technique to analyse the network data comprising of industrial operation. Additionally, the study has also applied time series based anomaly detection techniques in order to detect the attacks in the data. Two different ML algorithms such as RF and SVM has been used. Besides, the feature selection process has been deployed to predict the relationships in the input data and these selected features has supported in distinguishing the non-malicious and malicious instances. Thus, the SVM has been utilised to detect attacks of 35 different subtypes and seven different categories. This has projected that the combination of RF and SVM has been able to improve the detection capabilities of common industrial IDS. The study has produced 90% and 95% of accuracy in detection of attacks in the industrial networks. But, an enhanced level of security can overcome security threats. In contrast, an OLWPR (Online Locally Weighted Projection Regression) approach has been implemented for anomaly detection in WSN [27]. The study has been portrayed under three different phases such as data compression, prediction based on LWPR and dynamic thresholding technique to identify the anomalous data. As the data increases, the dimensions also increases. So, the data compression technique has been performed by PCA (Principle Component Analysis) for dimensionality reduction. Whereas, the LWPR is considered as the category of LWL (Locally Weighted Learning), which has been used under purely incremental learning and memory based LWL. The study has focused on purely incremental method called LWPR that has considered local model instead of global model. In this process, the prediction has been done by the weighted combination of local or linear model. After comparing the results of LWPR with other algorithms such as SMO (Sequential Minimal Optimisation), Gaussian and LR, it has been found that OLWPR produced better outcomes with 91% accuracy. However, the accuracy rate has been identified to be lesser and enhanced improvements in the study is found to be significant to tackle the anomaly intrusion. The figure.4, denotes the ML approaches used in intrusion detection of anomalies.

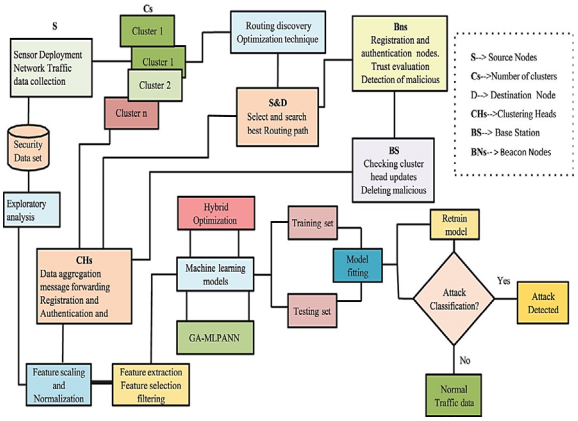

Figure 4. Intrusion Detection using Machine Learning Approaches [28]

5.2. Intrusion Detection System using Deep Learning

Several IDS has been introduced in order to provide security over big data and thus intrusion detection in computer networks in big datasets is significant. So, the suggested study [29] has employed CNN (Convolutional Neural Network) to monitor the security of internet. The IDS model has been implemented in which all the packet traffic present in the network has been classified. This has been classified based on benign and malignant classes. The model has been categorised into three different phases namely, convolutional, pooling and fully connected layers. Here, the feature extraction has been carried out by the convolutional and pooling layers, wherein the fully connected layer has performed the classification of classes. On convolutional layer, the input has been convolved by

using kernel map or feature detector. The features detectors has been represented as the matrices that has been applied to extract the shape, patterns, lines and some specific features from the input samples. After the process of feature detector, the feature maps has been produced, which has been mapped to the non-linear activation function. In case of pooling layer, the feature maps has been pooled to reduce the dimension and the purpose of this layer has to eliminate dependency on spatial location and noise. Additionally, the fully connected layer has been comprised of input, hidden and output neurons. These neurons helps in predicting the class to which the output neuron belongs. By involving these methods, the study has analysed the outcomes and has resulted better precision. Eventually, the study has possessed limitations of class imbalance of training dataset and insufficient number of minority attacks samples. Besides, to improve the accuracy of intrusion detection of network security communication, the considered study has deployed IDS based on MSCNN (Multi-Scale CNN) [30]. The two main contributions of the study has to perform feature extraction and to resolve compatibility issues arising among the NN and IDS. The feature extraction has been done by using data mining approach based on DL. The features has been extracted from the unordered data in order to enhance the precision of intrusion detection. Further, the compatibility related issues has been solved by applying MSCNN algorithm. This method has reduced the processing parameters and has thus increased the convergence speed. From analysis, it has been detected that the outcomes generated in terms of convergence speed by IDS based on MSCNN has been greater than the results produced by RNN (Recurrent Neural Network) and AdaBoost method. The average accuracy has been enhanced by 4.37% and average error detection has been decreased by 4.02%. This has denoted that the study has produced better results with improved detection accuracy.

As DL methods are regarded as the ideal solution for unstructured data issues, it is also a challenge to intimate that this technique is similarly applicable to the structured data. Hence, the intimated study [31] has developed DL and entity embedding based IDS in WSN. The DL method used in the study has been found to be end-to-end ANN (Artificial NN). Here, the study has considered the categorical values as features and then has mapped the features to m-dimensional vectors of continuous variables. This technique has made the raw features to be more robust representation and the mapping has been done by the NNs. The layers or weights present in the network model has been fine-tuned during backpropagation process, which has been done through a sequence of forward and backward iterations. Here, the weights of the network has been initialised by using statistical initialiser. Thus, the multi-layer ANN model has ensured learning of nonlinear boundaries to generate accurate classification. Further, the entity embedding technique has automatically learned the robust representation of raw features. To select the optimal combination of hyperparameters, the study has introduced grid search method. Therefore, the study has incurred better results in terms of evaluation scores. Similarly, the considered study [32] has intended in handling imbalanced attacks by using DNN (Deep NN). During normalisation, the input data has been transformed from categorical values into numerical values. Then by using cross correlation technique, the optimal features has been chosen applied to train the network. The reduction in computational complexity and dimension has been held by deploying cross correlation approach. These optimal features has been introduced into the input layer, which has been passed into the network in the forward direction. Based on the input layer, the hidden layer depends on the activation function and input vector size. Besides, the activation function has been present in the output layer that classifies the features of the input. Thus, the absolute outcome has denoted the type of attacks in the network with an average accuracy of 95.5%. But the study lacks in accuracy and computational complexity, if the number of attacks to be detected is increased.

Detecting and alleviating the intrusion is vital to make the network more reliable and flexible. This motivated the intimated study [33] to implement hybrid CNN-LSTM (CNN-Long Short Term Memory) algorithm in order to predict the attacks in WSN. The network has used both temporal and geographical information grasped from sensor data. In this case, CNN has been utilised to extract the features from sensors and thus learns the spatial information. The output of final CNN layer has been fed into LSTM layer, to detect long term patterns and the temporal dependencies. The memory cells present in LSTM network, allows them to retain and learn long term dependencies making it to capture temporal dependencies. Thus, the integration of both CNN and LSTM has involved the combination of output of both the networks and thus a unified representation of temporal and spatial information has been created. Here, the fusion layer has interlinked the components of CNN and LSTM to correlate the feature representation learned by each networks. Therefore, the study has efficiently implemented in allowing the model to familiarise the dynamic changes in WSN environment. However, the study has not focused on enhancing its ability to predict subtle attacks. Likewise, the suggested study [34] has employed DHN-SCA (Deep Hybrid Network with Spatial and Channel Attention), to effectively detect the evolving threats

and the unknown attack patterns in WSN. This study integrates the CNN with local attention module in order to optimise the efficiency and precision of IDS. The local attention model used in this study has been comprised of two sub-modules such as Spatial and Channel attention. The spatial attention model has deployed average pooling to feature tensor, whereas the channel attention module has applied global avg and global max pooling, then processed by fully connected layer. Further, element wise multiplication has been performed with original features to refine the feature tensor. The efficacy of the study has been evaluated in terms if performance metrics and has been compared with other intrusion detection methods.

Table 1. Comparative Analysis of Different AI techniques of Intrusion Detection in WSN

References	Objectives	Methodologies	Inference
[35]	The main motive of the study has to improve the accuracy and detection rate of intrusion. The study has also aimed in reducing the processing time.	The study has employed modified binary GWOSVM-IDS method, where 3, 5 and 7 wolves has been used to predict the best number of wolves. Here, the feature selection has been performed by modified binary GWO method to select the optimal feature set. Whereas, the SVM has been used for classification.	The overall performance of the study has relied on the prediction of unknown classes. Using more of wolves has also reduced the execution time. The results of the study has been analysed in terms of detection accuracy and rate, false alarm rate, detection rate, number of features and execution time. This has shown better accuracy rate in detection of attacks.
[36]	The objective of the study has to develop an intelligent IDS framework for improving the security if WSN.	The study has implemented CSGO and LSVM for accurately locating the intrusions from the given input IDS dataset. The study has undergone data pre-processing, feature selection and classification. The CSGO has been utilised in feature selection, to resolve the multi-objective optimisation issues. In addition, the LSVM for classification to distinguish intrusions.	As the CSGO technique has provided increased efficiency, convergence speed, optimal solution, the study has produced better feature selection process. On the other hand, the LSVM has overcome over-fitting issues, reduced computational complexity, increased speed, flexibility and scalability. Thus, the performance of the study has been found to be improved.
[37]	To apply the intelligent based model to automate the intrusion detection has been the main aim of the study	A ML based MR-IMID has been utilised in the study to predict the intrusions on the network along with several data classification tasks. This method has processed large datasets by employing commodity hardware and the multiple network sources has been deployed.	The MR-IMID method has been used to detect the intrusions. The intrusion has been predicted by unknown test scenarios and has stored the data to reduce the inconsistencies. The accuracy of intrusion detection has been identified to be 97.7% and 95.7%.
[38]	The main objective of the study has to improve the IDS using DL techniques	The study has employed hybrid method of CNN and LSTM to produce enhanced intrusion detection.	The outcomes produced by the study has been evaluated based on precision, recall, false positive and F1 score and has produced 99.70% accuracy.
[39]	The aim of the study has to provide security in data communication	To improve and produce security in data communication, a feature selection algorithm known as linear correlation coefficient and conditional random field has been implemented. This has been done to choose the most supported features and then distinguish by deploying CNN.	The study has been evaluated and has incurred 98.88% detection accuracy. To validate the performance of the study, the system has been evaluated in tenfold cross validation.

[40]	The determination of unknown attacks in WSN by selecting relevant features has been considered as the main motive of the study	An enhanced empirical based component analysis has been employed to choose the relevant features. Combination of both empirical mode decomposition and PCA has been done to select most correlated features. Wherein, LSTM has performed the classification of selected features.	The system has been evaluated on four different datasets and thus compared with other methods. The outcomes has projected that the performance of the system has found to be enhanced.
# Abbreviations GWOSVM-IDS (Grey Wolf Optimiser with Support Vector Machine-Intrusion Detection System) CSGO (Chicken Swarm- Greedy Optimisation) LSVM (Likelihood SVM) MR-IMID (Map Reduce based Intelligent Model for Intrusion Detection)			

6. Research Gaps and Future Scope

1. The study has employed modified binary GWOSVM-IDS method to increase the detection accuracy of intrusion. But the study has not focussed on predicting the location of wolves, which helps in increasing the performance of GWO algorithm. Further, the detection rate and performance of classification process should be improved [35].
2. A CNN based intrusion detection has been used in the study and must be extended by improving the model by resolving class imbalance issues. This can be overcome by using automated methods to prevent biased classification decisions. Still, the improvement in detection accuracy of innovative cyber-attacks has to be done [29].
3. The study implemented MR-IMID, to automate the intrusion detection and has been introduced to perform multiple data classification. The study has produced an accuracy of 95.7% during validation process. Though the method predicted the unknown test scenarios, it lacks in providing increased detection accuracy. Still enhancement in precision can be involved to avoid inconsistencies of keenly predicting the intrusions [37].

6.1 Future Scope

The primary aim of the study is to project the various security attacks and AI based techniques that overcome the issues related with intrusion detection are replicated. The methodology, performance, strengths and limitations of studies are provided in a way to enhance the detection rate and accuracy of the system. Thus tend to help future researchers to have a knowledge on developing new features that can be incorporated into the conventional models, thus improving detection abilities. The challenges faced by the existing studies are interpreting new characteristics or patterns of dynamic environment in WSN, to predict potential intrusions. Further, the techniques implemented in these studies were less capable of analysing the different aspects of network security. Some recommendations provided by reviewing different studies are as follows,

- An important aspect is the reduction of computational complexity of the algorithms. This includes the exploration of new techniques and algorithms, which decreases the memory requirements and processing time of the system. The objective is to create a model with improved scalability and efficiency, so that it can be applied in a large scale network environment with minimum impact in the performance.
- The models should be able to adapt to the dynamically changing environments of the network and need to detect the malicious intrusions in real-time circumstances. So, sufficient resources are required to analyse the effectiveness of the models.
- Overall, the future work of researches should focus on developing new techniques and features to enhance the performance of IDS in WSN. Besides using stand-alone methodology provided reduced efficiency, wherein hybrid or combination of one or more algorithms tend to produce optimised performance and improved detection accuracy of malicious intrusions. This in turn extends by providing superior security affluence in the WSN environment.

7. Conclusion

In real-time scenarios, the WSN is applied in different areas including healthcare, industries, military, environmental and commercial applications. With wide applications, there is an emergence of intrusions in the network targeting to destroy the WSN environment. So, it is significant to analyse the recent techniques involved in detecting anomalies. Hence, the present study presented a survey on IDS deployment strategies in WSN. The overall review provided a complete understanding of what are WSN, security threats in WSN, AI techniques involved in intrusion detection. Moreover, the comparative analysis of various ML and DL based algorithms was signified projecting the different methodologies employed in predicting the intrusion of anomalies. The paper also focussed on the research gaps produced by exiting studies and recommendations for future researches to produce effective strategies of intrusion detection was also provided.

Declarations

Conflict of Interest

There is no conflict of interest.

Funding Support

There is no funding support for this study.

References

[1] D. Kandris, C. Nakas, D. Vomvas, and G. Koulouras, "Applications of wireless sensor networks: an up-to-date survey," *Applied system innovation,* vol. 3, no. 1, p. 14, 2020.

[2] R. Sarath Kumar, P. Sampath, and M. Ramkumar, "Enhanced Elman Spike Neural Network fostered intrusion detection framework for securing wireless sensor network," *Peer-to-Peer Networking and Applications,* pp. 1-15, 2023.

[3] C. Nakas, D. Kandris, and G. Visvardis, "Energy efficient routing in wireless sensor networks: A comprehensive survey," *Algorithms,* vol. 13, no. 3, p. 72, 2020.

[4] A. Khraisat, I. Gondal, P. Vamplew, and J. Kamruzzaman, "Survey of intrusion detection systems: techniques, datasets and challenges," *Cybersecurity,* vol. 2, no. 1, pp. 1-22, 2019.

[5] R. Zhang and X. Xiao, "Intrusion detection in wireless sensor networks with an improved NSA based on space division," *Journal of Sensors,* vol. 2019, 2019.

[6] R.-H. Dong, H.-H. Yan, and Q.-Y. Zhang, "An Intrusion Detection Model for Wireless Sensor Network Based on Information Gain Ratio and Bagging Algorithm," *Int. J. Netw. Secur.,* vol. 22, no. 2, pp. 218-230, 2020.

[7] S. Jiang, J. Zhao, and X. Xu, "SLGBM: An intrusion detection mechanism for wireless sensor networks in smart environments," *IEEE Access,* vol. 8, pp. 169548-169558, 2020.

[8] M. Adil, M. A. Almaiah, A. Omar Alsayed, and O. Almomani, "An anonymous channel categorization scheme of edge nodes to detect jamming attacks in wireless sensor networks," *Sensors,* vol. 20, no. 8, p. 2311, 2020.

[9] O. I. Khalaf and B. M. Sabbar, "An overview on wireless sensor networks and finding optimal location of nodes," *Periodicals of Engineering and Natural Sciences,* vol. 7, no. 3, pp. 1096-1101, 2019.

[10] A. Sarkar and T. Senthil Murugan, "Cluster head selection for energy efficient and delay-less routing in wireless sensor network," *Wireless Networks,* vol. 25, pp. 303-320, 2019.

[11] A. S. Toor and A. Jain, "Energy aware cluster based multi-hop energy efficient routing protocol using multiple mobile nodes (MEACBM) in wireless sensor networks," *AEU-International Journal of Electronics and Communications,* vol. 102, pp. 41-53, 2019.

[12] B. Bhushan and G. Sahoo, "Requirements, protocols, and security challenges in wireless sensor networks: An industrial perspective," *Handbook of computer networks and cyber security: principles and paradigms,* pp. 683-713, 2020.

[13] D. E. Boubiche, S. Athmani, S. Boubiche, and H. Toral-Cruz, "Cybersecurity issues in wireless sensor networks: current challenges and solutions," *Wireless Personal Communications,* vol. 117, pp. 177-213, 2021.

[14] H. A. Babaeer and S. A. Al-Ahmadi, "Efficient and secure data transmission and sinkhole detection in a multi-clustering wireless sensor network based on homomorphic encryption and watermarking," *IEEE Access,* vol. 8, pp. 92098-92109, 2020.

[15] Z. Chiba, N. Abghour, K. Moussaid, A. El Omri, and M. Rida, "New anomaly network intrusion detection system in cloud environment based on optimized back propagation neural network using improved genetic algorithm," *International Journal of Communication Networks and Information Security,* vol. 11, no. 1, pp. 61-84, 2019.

[16] S. Venkatraman and B. Surendiran, "Adaptive hybrid intrusion detection system for crowd sourced multimedia internet of things systems," *Multimedia Tools and Applications,* vol. 79, no. 5-6, pp. 3993-4010, 2020.

[17] H. Bai, X. Zhang, and F. Liu, "Intrusion detection algorithm based on change rates of multiple attributes for WSN," *Wireless Communications and Mobile Computing,* vol. 2020, pp. 1-16, 2020.

[18] T. Ghazal, "Data Fusion-based machine learning architecture for intrusion detection," *Computers, Materials & Continua,* vol. 70, no. 2, pp. 3399-3413, 2022.

[19] A. F. J. Jasim and S. Kurnaz, "New automatic (IDS) in IoTs with artificial intelligence technique," *Optik,* vol. 273, p. 170417, 2023.

[20] A. B. Abhale, "Deep Learning Perspectives to Detecting Intrusions in Wireless Sensor Networks," *International Journal of Intelligent Systems and Applications in Engineering,* vol. 11, no. 2s, pp. 18-26, 2023.

[21] M. Aljebreen *et al.*, "Binary Chimp Optimization Algorithm with ML Based Intrusion Detection for Secure IoT-Assisted Wireless Sensor Networks," *Sensors,* vol. 23, no. 8, p. 4073, 2023.

[22] S. Subbiah, K. S. M. Anbananthen, S. Thangaraj, S. Kannan, and D. Chelliah, "Intrusion detection technique in wireless sensor network using grid search random forest with Boruta feature selection algorithm," *Journal of Communications and Networks,* vol. 24, no. 2, pp. 264-273, 2022.

[23] H. Tabbaa, S. Ifzarne, and I. Hafidi, "An online ensemble learning model for detecting attacks in wireless sensor networks," *arXiv preprint arXiv:2204.13814,* 2022.

[24] P. KANAGAVALLI and D. KARTHIKEYANI, "INVESTIGATION OF INTRUSION DETECTION SYSTEM USING RANDOM FOREST, CART AND PROPOSED SECURE RANDOM FOREST ALGORITHMS (SRFA)," *Journal of Theoretical and Applied Information Technology,* vol. 101, no. 3, 2023.

[25] X. Tan *et al.*, "Wireless sensor networks intrusion detection based on SMOTE and the random forest algorithm," *Sensors,* vol. 19, no. 1, p. 203, 2019.

[26] S. D. D. Anton, S. Sinha, and H. D. Schotten, "Anomaly-based Intrusion Detection in Industrial Data with SVM and Random Forests," *arXiv preprint arXiv:1907.10374,* 2019.

[27] I. G. A. Poornima and B. Paramasivan, "Anomaly detection in wireless sensor network using machine learning algorithm," *Computer communications,* vol. 151, pp. 331-337, 2020.

[28] G. G. Gebremariam, J. Panda, and S. Indu, "Design of advanced intrusion detection systems based on hybrid machine learning techniques in hierarchically wireless sensor networks," *Connection Science,* vol. 35, no. 1, p. 2246703, 2023.

[29] S. Ho, S. Al Jufout, K. Dajani, and M. Mozumdar, "A novel intrusion detection model for detecting known and innovative cyberattacks using convolutional neural network," *IEEE Open Journal of the Computer Society,* vol. 2, pp. 14-25, 2021.

[30] J. Yu, X. Ye, and H. Li, "A high precision intrusion detection system for network security communication based on multi-scale convolutional neural network," *Future Generation Computer Systems,* vol. 129, pp. 399-406, 2022.

[31] B. Almaslukh, "Deep Learning and Entity Embedding-Based Intrusion Detection Model for Wireless Sensor Networks," *Computers, Materials & Continua,* vol. 69, no. 1, 2021.

[32] V. Gowdhaman and R. Dhanapal, "An intrusion detection system for wireless sensor networks using deep neural network," *Soft Computing,* pp. 1-9, 2021.

[33] T. Gopala, V. Raviram, and U. K. NL, "Detecting Security Threats in Wireless Sensor Networks using Hybrid Network of CNNs and Long Short-Term Memory," *International Journal of Intelligent Systems and Applications in Engineering,* vol. 12, no. 1s, pp. 704-722, 2024.

[34] V. Gatate and J. Agarkhed, "Enhancing Intrusion Detection in Wireless Sensor Networks through Deep Hybrid Network Empowered by SC-Attention Mechanism," 2023.

[35] M. Safaldin, M. Otair, and L. Abualigah, "Improved binary gray wolf optimizer and SVM for intrusion detection system in wireless sensor networks," *Journal of ambient intelligence and humanized computing,* vol. 12, pp. 1559-1576, 2021.

[36] D. Hemanand, G. V. Reddy, S. S. Babu, K. R. Balmuri, T. Chitra, and S. Gopalakrishnan, "An intelligent intrusion detection and classification system using CSGO-LSVM model for wireless sensor networks (WSNs)," *International Journal of Intelligent Systems and Applications in Engineering,* vol. 10, no. 3, pp. 285–293-285–293, 2022.

[37] M. Asif, S. Abbas, M. Khan, A. Fatima, M. A. Khan, and S.-W. Lee, "MapReduce based intelligent model for intrusion detection using machine learning technique," *Journal of King Saud University-Computer and Information Sciences,* 2021.

[38] M. Ahsan and K. E. Nygard, "Convolutional Neural Networks with LSTM for Intrusion Detection," in *CATA*, 2020, vol. 69, pp. 69-79.

[39] B. Riyaz and S. Ganapathy, "A deep learning approach for effective intrusion detection in wireless networks using CNN," *Soft Computing,* vol. 24, pp. 17265-17278, 2020.

[40] L. Zhiqiang, G. Mohiuddin, Z. Jiangbin, M. Asim, and W. Sifei, "Intrusion detection in wireless sensor network using enhanced empirical based component analysis," *Future Generation Computer Systems,* vol. 135, pp. 181-193, 2022.