International Journal of Mechanical Engineering

Dense Net RNN – An Intrusion Prevention System to Mitigate DoS Attacks in Wireless Sensor Networks

A.Sarkunavathi

Research Scholar ,Department of Information Technology

Annamalai University Annamalai Nagar, India

Dr.V.Srinivasan

Professor, Department of Information Technology

Annamalai University Annamalai Nagar, India

Dr.M.Ramalingam

Professor& Head Department of Information Technology

Mailam Engineering College, Anna University

Mailam, India

Abstract:

The widespread application of the Wireless Sensor Networks (WSNs) in many areas of network has increased the network prone to various security threats. The threats are attacks that incapacitate the effective operational of the network. One form of such attack is the Denial of Service (DoS) attack that gets through all the layers of the WSN. In this paper, an Intrusion Prevention System is developed that declines the rate of DoS attacks in WSN. The system uses Dense Neural Network (Dense Net) algorithm, which is trained with the training datasets to develop itself as a model for validating the attacks in WSN. This Prevention System is also examined by using performance metrics of different machine learning classification categories such as Support Vector Machine (SVM), Naïve Bayes (NB), Artificial Neural Networks (ANN) on NSL-KDD dataset in different sizes**.** From these classification categories the Dense net Recurrent Neural Network (Dense Net RNN) model trained detects the attack from the test dataset of DoS attack dataset. The simulation is conducted to test the efficacy of the model and the results shows that the Dense Net base RNN model is effective in increasing the detection and prevention rate than other existing deep learning models.

Keywords: Wireless Sensor Networks, Denial of Service, intrusion prevention system, Dense Net

1. Introduction

Wireless sensor networks (WSNs) are a hot topic in both the scientific and non-scientific worlds. Because of the rapid growth of the WSN, new possibilities and problems arise all the time. Vulnerabilities in network devices may allow attackers to assemble a large number of nodes for such attacks as the number of network devices grows. Sensors will become unreachable if the attack is strong enough, and genuine users will be unable to use them. Hackers can try to sneak in through the back door as this powerful strain takes control of devices. That is why security must be integrated into wireless sensor networks from the start; it must serve as the WSN settings, requiring stringent validity checks, data verification, and authentication, in addition to encryption of all communications. The security threats posed by sensors cannot be overstated in view of their critical role.

Even so, conducting actual tests with Denial-of-service attacks is difficult due to the large geographic spread of attack sources and the fact that trials conducted on a local network may not be sufficient to demonstrate the real scenario. It is tough to gather a sufficient number of infected and ready-to-attack workstations in the lab since DoS attacks require a large number of managed devices. Instead of actually executing Denial-of-service attacks, several modelling methodologies and tools can be used to examine them. Through the use of modelling, it is possible to estimate the impact of various attack properties while using significantly fewer resources. It serves as a proving ground for comparing the financial and operational impact of various attack and defense scenarios.

Weaknesses in the WSN make it vulnerable to both external and internal attacks. As a result, it must meet certain security requirements drawn from the context of the application in order to function. When it comes to WSN security, it is a laborious endeavour that must balance many competing objectives at once, such as scalability and functionality. A multilevel analysis is critical since it helps to clarify the security risk problem and gives several perspectives on how to approach it.

The paper is structured as : The Related works suggesting about different intrusion prevention system in machine learning as well as deep learning followed by the different attack profiles in WSN as well as the IoT networks and brief about the Dense Net architecture is described. Then, the proposed Dense Net RNN and experiment analysis is made over the dataset, which is trained with the training datasets to develop itself as a model for validating the attacks in WSN. The simulation is conducted to test the efficacy of the model and the results show that the Dense Net model is effective in increasing the detection and prevention rate than other existing deep learning models. This paper is finally concluded in section conclusions.

2. Related works

DoS attacks aren't new; they've been discussed in the literature for a long time. However, there are numerous conflicting viewpoints on the subject of this form of attack. A full taxonomy of DoS attacks is provided by certain writers who look at DoS attacks from the OSI or TCP/IP reference model point of view. The denial-of-service attacks can be studied using a variety of modelling techniques [1-5], while others focus on detection and prevention.

Despite the abundance of DoS literature, only a few researchers have attempted to formalise DoS attacks on wireless sensor networks [6-9]. A series of conditions is created in this paper so that, allow an in-depth and extensive evaluation of proposed methodology in terms of their utility and efficiency, allowing all current approaches to denial-of-service formal modelling to be compared and arranged if the criteria are met. To be deemed a useful, practical, and effective framework, the modelling technique must have a specific set of characteristics.

For the prevention of denial-of-service (DoS) attacks, writers in [6] suggested an approach that incorporates a cryptographic mechanism and a clustering method. The Analytical Representation criterion is met since the mechanism is described as a series of structured processes. Researchers in the publication fail to mention whether or not the proposed mechanism can be used in other situations. Scientists talk about energy evaluation in their work and share performance data. It is a Multidimensional technique with some flexibility, scalability, and consistency.

Scientists have developed and demonstrated the working model may be used to find protocol vulnerabilities in [7] a formal framework for modelling semantic DoS attacks on wireless networks when it comes to DDoS modelling. For them, formal description and analysis are the only ways to go about things. Although the approach is scalable, it is also rather rigid. However, the authors fail to discuss Energy Evaluation while considering and introducing the cost model. Multilevel Analysis, too, is dissatisfied, as we've seen with earlier examples.

The author in [8] proposes another way that makes use of algorithms. For the prevention of denial-of-service (DoS) attacks, the authors developed a new Message Observation Mechanism (MoM). In order to identify frequency attacks and content attacks, this technique uses a similarity function based on spatio-temporal correlation. While all procedures for reroute and rekeys are discussed in the text, the approach is both scalable and adaptable. There are no other dimensions of analysis mentioned by the authors despite the fact that they mention Energy Evaluation. The suggested mechanism does not meet the Universality criterion because it is tailored to wireless sensor networks.

Waizarali et al. [10] Proposed a Machine learning based approach for detecting the DoS attacks in the WSN. The test is performed over K-Nearest Neighbor (KNN), Logistic Regression (LR), Support Vector Machine (SVM), Gboost, Decision Tree (DT), Naïve Bayes, Long Short-Term Memory (LSTM), and Multi-Layer Perceptron (MLP) with the WSN-DS dataset. From these Gboost algorithm which is an enhancement of DT proved that the statistical and logical classification categories performed the best on numeric statistical dataset and has lower execution time.

Wu et al. [11] proposed a Long Short-Term Memory (LSTM) based Learning with Bayesian and Gaussian Processing to detect the anomalies in the industrial based IoT networks. They use back propagation which helps in the solving the main issue found in the RNN called the vanishing gradient problem. This system classifies, process and forecast the anomalies by using their real -life time series-based dataset from the sensors such Land, Power and the Loop sensor.

Mohd et al. [12] proposed a Novel Intrusion Detection System based on SVM. In order to achieve improved outcome this system is technologically advanced and tested by using several kernel functions such as redial, sigmoidal and the linear functions. The Association rule set is applied over the raw data set from the Opnet modeler 17.5 in a noisy environment and achieved higher accuracy with the radial function. This system is best suited detection of the denial of sleep attack. But this system couldn’t handle the other types of Denial-of-Service attacks.

Yadav at al. [13] proposed a system that can identify and mitigate DoS attacks in wireless sensor networks. The RNN is used as the classifier for this proposed model. The verification is made by 10-fold cross validation in nine iterations and used WSN-DS dataset for the evaluation of the false positive alarm rates. This model provides an accuracy of 99.8% with a 0.3 percent positive defect rate.

As the WSN are resource constrained Borgiani et al. [14] proposed D-ConCReCT a distributed and congestion control by means of the duty-cycle restriction than can detect as well as alleviate the DoS attacks even in large scale WSN networks and Industrial IoT networks. The curb of this approach is dearth of the dynamic detection levels in threshold.

While designing an Intrusion detection system for DoS attacks in WSN the energy constraint is also an important feature to be taken into account, so to make this Suryaprabha et al. [15] proposed an optimized algorithm called OBES which is simulated in NS2 attains less delay in network as well as energy consumption leading to increased lifetime for the WSN network.

A denial-of-service attack model that combines multiple types of attacks as well as several types of resource exhaustion for an accurate portrayal of an attack does not yet exist when it comes to denial-of-service attacks[15]. Denial of service attacks should be detected, defended against, and mitigated using systematic, standardised, and organised approaches. Dealing with DoS requires a multidimensional, in-depth approach that includes applying logical formulae to examine a variety of factors of the attack as a whole.

Until now, Quality of Protection Modeling Language (QoP-ML) has been the only modelling language to meet all of these criteria at once, according to the author research. It allows for security to be balanced against system efficiency, multicriteria analysis to be performed, and the ability to describe the environmental conditions in detail to be expanded. It is feasible to assess the required level of protection and then adjust the security measures to fulfil those requirements while also ensuring that the system operates at maximum efficiency.

The Automated Quality of Protection Analysis tool can help with this type of in-depth analysis by evaluating the influence of each operation indicated in the prepared security model on the overall security of the system. Furthermore, in prior studies, methodologies were proposed and studied that were also successful in evaluating the analysed IT environments' time, energy, security, financial costs, and environmental impact all at the same time. To create a network model, use the Quality of Protection Modeling Language, the type of device, the communication medium type and features, the network topology, and packet flow can all be considered, and observe how different combinations of these components affect the likelihood of a DoS success.

3. Attack Profiles

In an IoT-connected home or WSN, there could be loads or even hundreds of sensors, each detecting somewhat diverse. Most of these devices can't make a direct connection to the Internet since other protocols are used to connect to them. As a result, the IoT gateway is critical, as this device can aggregate and process sensor data before it is sent to Internet servers for storage. As there are many other ways to attack the sensor nodes as well as the computer on the network, some of the attacks that happens in the sensor as well as IoT network are given below.

Denial-of-Service Attacks

A DoS attack seeks to overload systems and deny service to some or all legitimate requests by flooding the targeted computer or resource with excessive requests. It is impossible to thwart a DoS attack by blocking a single source when the inbound traffic overwhelming the target originates from several separate places. Some DoS attacks aim to bring a service on the victim host to a halt from the outside. For example, Ping-of-death attack, the attacker attempts to bring down the target system by sending a large ping packet to it in the hopes that it will fail to handle the incoming data.

In the Internet of Things, low-rate wireless personal area networks (PANs) are a frequent method for device communication. Strict hardware cost, power consumption and memory usage constraints have resulted in a slew of security flaws. These vulnerabilities include traffic eavesdropping, packet replay, and collision attacks. Depleting the WSN energy supply is a straightforward attack strategy. It is important to note that some attacks, such as vampires, are actually routing-layer resource exhaustion attacks that are designed to deplete a network node completely. Deny-of-sleep attacks can take many forms.

Sleep Deprivation Attack: In order to lengthen the lifespan of the network, sensor nodes that can go into a low-power sleep mode come in handy. It is possible that the attacker uses a sleep deprivation attack to drastically reduce the lifetime of a target device by communicating with it in a way that appears genuine, the attacker's purpose, on the other hand, is to prevent the victim node from entering power-saving sleep mode

Barrage Attack: The assailant attempts in order to keep the victim awake by bombarding it with seemingly legitimate requests. Though they are issued at a considerably faster rate, the requests have the goal of making the victim execute labor-intensive tasks. Sleep deprivation assaults are more difficult to detect than barrage attacks since they are carried out solely through the use of seemingly pleasant contacts.

Broadcast Attack: Suspicious nodes can send unauthenticated traffic and extended messages to other nodes, which must be received before being denied owing to a lack of authentication. Because such assaults have little effect on system throughput and nodes that receive them waste energy, they are difficult to detect. As a result, they're difficult to spot.

Proposed Model

4.1 Dense Net Architecture

Dense Net (Dense Convolutional Network) is an architecture that uses shorter connections between layers to deepen deep learning networks while also making them more effective to train. The Dense Net is a convolutional neural network that connects all layers (with matching feature-map sizes) to each other directly using dense blocks,

The Dense Net is a sort of convolutional neural network that uses dense blocks to link all layers (with matching feature-map sizes) directly to each other, as a result, there are a lot of connections between the layers. Traditional n-layer convolutional networks have n connections, one between each layer and the one after it.

Each layer in Dense Net links to every other layer in a feed-forward manner, resulting in a total of n(n+1)/2 connections. The layers in between the input and output are interconnected with each other like first layer connected to second and the remaining layers ,and the second layer connected to the next layer and so on. This is done to ensure that the maximum quantity of data can be transmitted between the tiers of the network. Each layer gets input from all previous levels and passes on its own feature maps to all subsequent layers to keep the system's feed-forward nature.

The elimination of the vanishing-gradient problem, enhanced feature propagation, feature reuse, and a large reduction in the number of parameters are all appealing features of Dense Nets. The vanishing gradient problem is an issue that describes how gradients aren't properly back-propagated to the network's original layers as networks become deeper. As one moves backwards into the network, the gradients get smaller, and the earliest layers lose their ability to learn basic low-level characteristics. To address this issue, several architectures have been designed such as Res Net, Highway Networks, Fractal Nets, and Stochastic depth networks.

These networks, regardless of their architectural principles, all attempt to build channels for information to flow between the initial and final layers. With the same goal in mind, Dense Nets establish path between the layer of networks.

Aside from the basic convolutional and pooling layers, the Dense Net has two crucial blocks.

Dense Net consists of two important blocks other than the basic convolutional and pooling layers. Dense Blocks and Transition Layers are the two types of Dense Blocks. A basic convolution and pooling layer are the foundation of the Dense Net. Next to that is a transition layer which is continued by the dense block and again it continues for another two layers and at last is another dense block continued with classification layer.

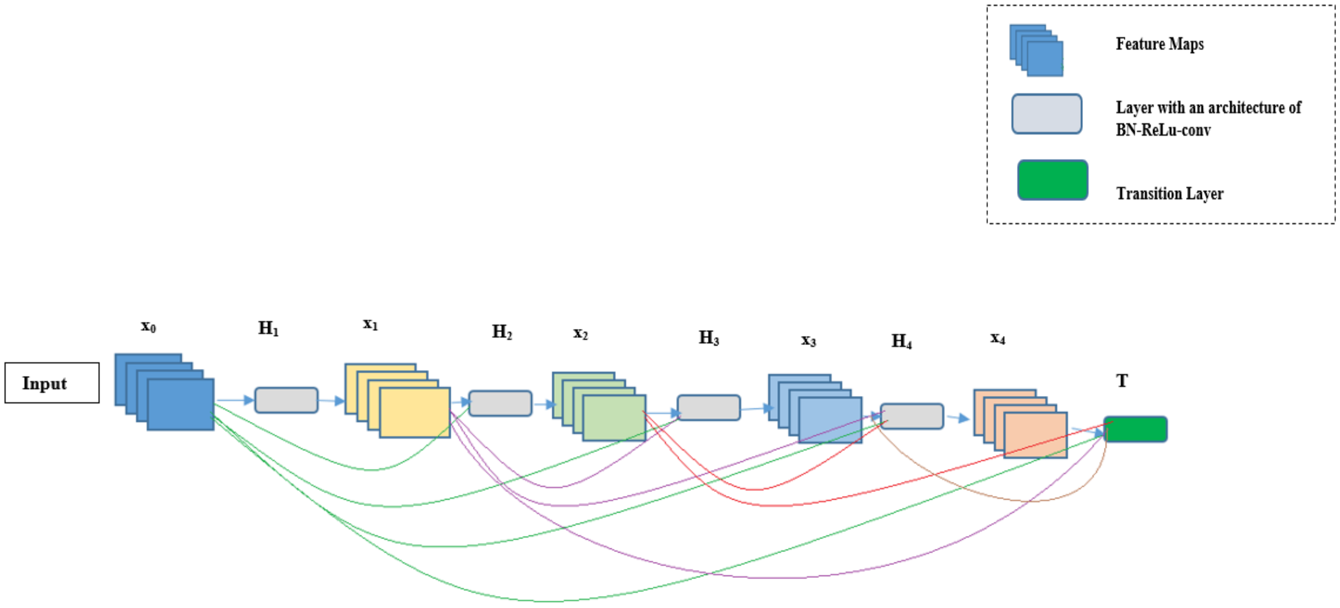

Figure 1. A dense 5-layer block with a k=4 growth rate. Each layer takes all of the feature maps before it as input.

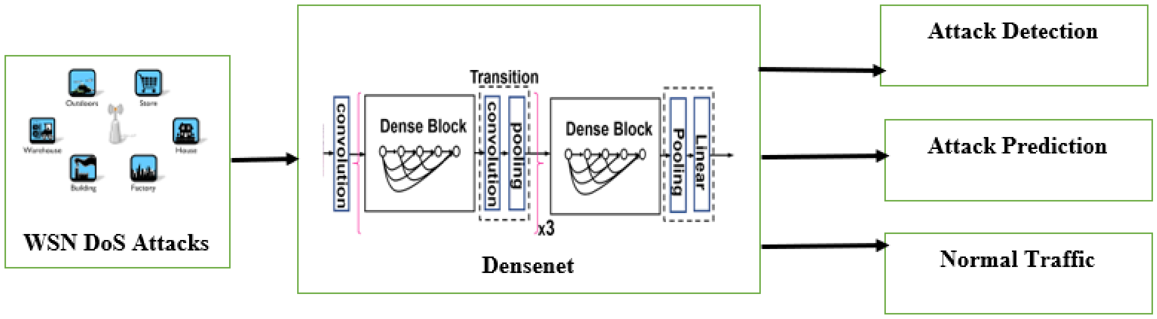

Figure 2. Densnet based deep learning technique Intrusion Detection and Prevention System

The Figure 2 depicts the components of the Densnet based deep learning technique Intrusion Detection and Prevention System. The deep learning based technique are more efficient in detecting the attacks because they can intelligently predict the future unknown attacks which are often different from previous attacks through learning from the existing legitimate samples of network traffic. It is critical to fine-tune hyperparameters when training a deep learning model. The proposed model includes hyperparameters such as growth rate (K), dropout, network depth, number of dense blocks, learning rate, weight decay, optimizer, momentum, epochs, batch size, and weight regularisation.

4.2 Modified Densenet RNN with deep Learning

In DenseNets, a dense cluster consists of *n* identical cells. Interactions between the soma and the cytosol cause inhibitory spike trains to travel to each cell at a rate of *x*, and these spike trains follow a pattern determined by random selection of interactions. Assume *q* is the chance that a cell in the cluster will be in an activated state in the steady state. Based on previous research, it is possible to derive a numerical solution for *q* such that

$$q=\varsigma(x)=-\frac{(c-nx)+\sqrt{4p(\lambda^{-}+x)(n-1)d-(c-nx)^{2}}}{2p(\lambda^{-}+x)(n-1)}$$

with

$c = rp+\lambda^{+}p-r-\lambda^{-}n- npr-\lambda^{+}pn$,

$d = n\lambda^{+}$

where

p - Probability of repeated-firing if a cell tries to fire,

r - Cell firing rate,

In a cell, *r* represents the firing rate, while in the external world, λ^{+} and λ^{-} represent excitatory and inhibitory spikes, respectively. For vectors and matrices, the term-by-term function $\zeta(\cdot)$ is used for notation ease.

In multi-layer architectures, denseNets are built as follows: A activation of quasi-linear cells q(x) = min(x,1) occurs in the DenseRNN first layer, where the external sources deliver excitant spike trains to RNN cells.Cells in the preceding layer provide inhibitory spike trains to cells in the subsequent *L* layer, which results in an activation function for cells in the latter layer, with $q(x) = \zeta(x)$. In the last layer, we have an RNN-ELM. DenseNets with an *L*-hidden layer ($L\geq2$) have weight matrices $W_1,\cdots, W_L \geq$ and W_{L+1} as the linking weight matrices between the layers. With input *X*, DenseNet forward pass on *X* is defined as follows:

$$X=\begin{cases} Q_1=\min(X,1) & for\ l=1 \\ Q_l=\varsigma(Q_{l-1},W_{l-1}) & for\ l=2,3,\ldots,L+1 \\ O=Q_{l+1}W_{l+1} & otherwise \end{cases}$$

where

Q_1 - output of 1st layer,

Q_l - output of lth layer and

O - DenseRNN output.

Work in [13,14,16] created an effective training approach for DenseRNN that fuses unsupervised and supervised learning techniques in order to estimate the values of $W_1,\cdots, W_L \geq$ and W_{L+1} for training datasets with $\{(x_n, y_n)|n = 1,\cdots,N\}$.

Steps Involved in Proposed Model Development:

The factors of the deep learning algorithms influence classification performance including the number of classifications as well as the hidden nodes, numerous hidden layers and optimization methods. The steps involved in this proposed model using deep learning algorithms are:

Step 1: The datasets for training and testing should be normalised.

Step 2: Train the deep learning models with a a number of layers, as well as validation data. Fine-tune the factors of deep learning models.

Step 3: Examine the deep learning patterns for accuracy.

Step 4: Assess the correctness of the models.

Comparing to our previous work on Generative Adversarial Network that uses recurrent neural network at its discriminator network to maximising discrimination and reducing the errors to a minimum level. Likewise, the DenseNets uses recurrent neural network at its last layer to reduce the detection errors.

4. Results and Discussions

In this section, the performance of the model is compared with existing methods in terms of various machine learning models SVM, NB and ANN. The study is made over the (NSL-KDD) datasets available at https://www.kaggle.com/hassan06/nslkdd/activity to test the efficacy of the model and the datasets with the details of DoS are used to train the classifier. The NSL-KDD dataset is divided into two sections: the first one is KDDTrain+, which is a CSV file containing the entire training dataset, labelled with attack kinds and complicated levels, the other is KDDTest+, a CSV file containing the whole testing dataset with attack categories and complicated levels

Dataset	R2L	U2R	Probe	DoS	Normal	Instances
KDD Train+	**995**	**52**	**11656**	**45927**	**67343**	**125973**
KDD Test+	**2885**	**67**	**2421**	**7460**	**9711**	**22544**

Table 1. NSL-KDD distribution of normal and attack records.

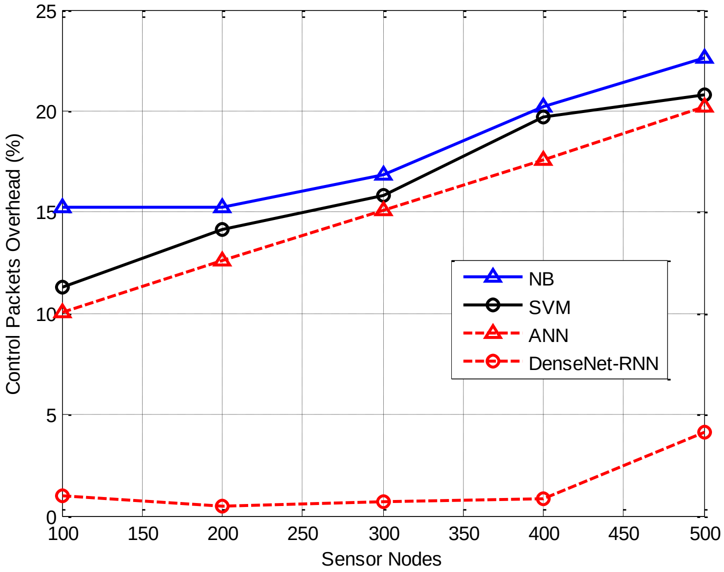

Figure 3: Control Packets Overhead

Figure 3 shows the results of control packets overhead between DenseNet-RNN and existing ML models over jamming attack mitigation. The results of simulation shows that the DenseNet-RNN obtains reduced control packets overhead than other methods.

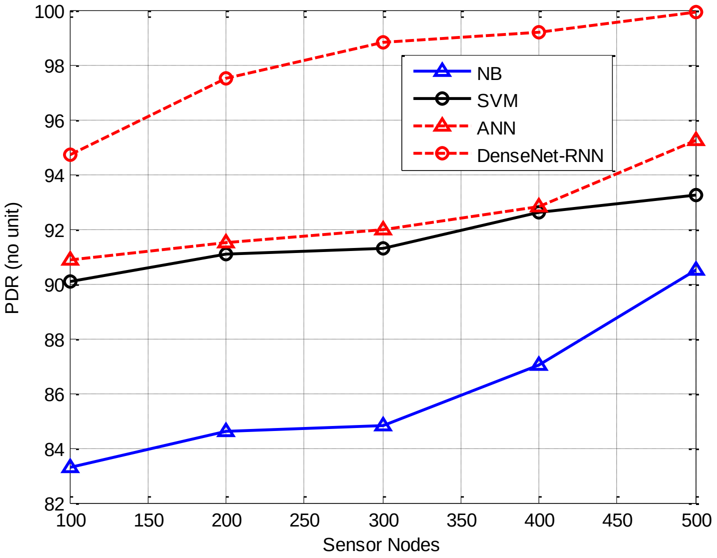

Figure 4: Packet Delivery Rate

Figure 4 shows the results of Packet Delivery Rate between DenseNet-RNN and existing ML models over jamming attack mitigation. The results of simulation shows that the DenseNet-RNN obtains increased rate of packet delivery ratio than other methods.

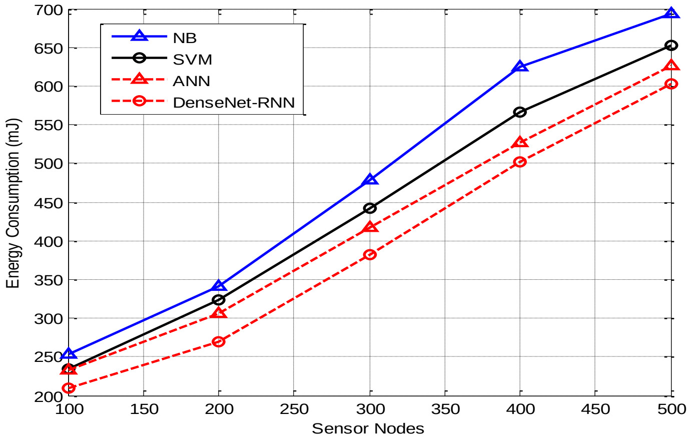

Figure 5: Energy Consumption

Figure 5 shows the results of Energy Consumption between DenseNet-RNN and existing ML models over jamming attack mitigation. The results of simulation shows that the DenseNet-RNN obtains reduced energy consumption than other methods.

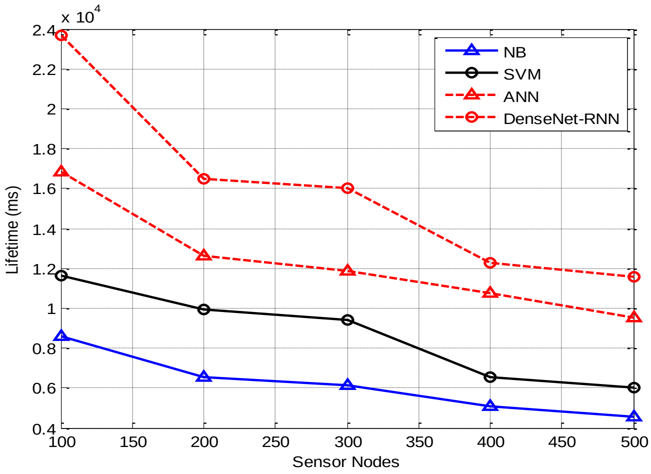

Figure 6: Network Lifetime

Figure 6 shows the results of Network Lifetime between DenseNet-RNN and existing ML models over jamming attack mitigation. The results of simulation shows that the DenseNet-RNN obtains increased rate of network lifetime than other methods.

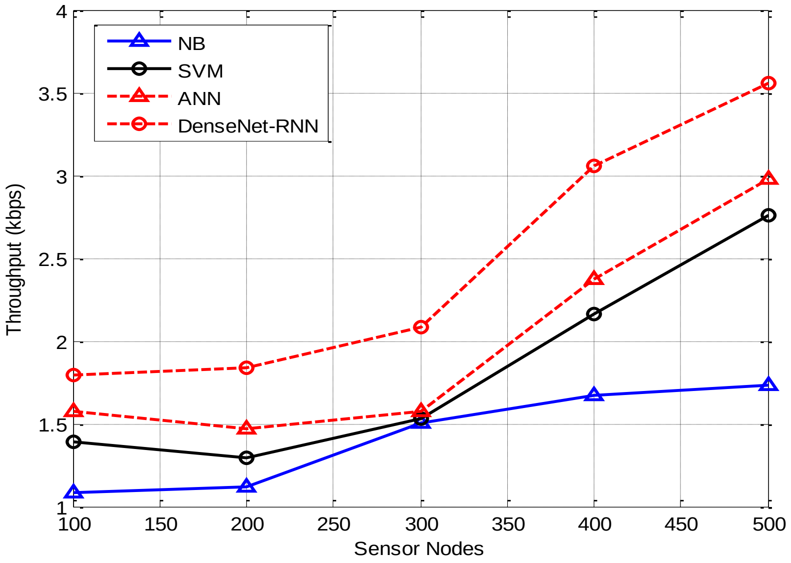

Figure 7: Throughput

Figure 7 shows the results of Throughput between DenseNet-RNN and existing ML models over jamming attack mitigation. The results of simulation shows that the DenseNet-RNN obtains increased rate of throughout than other methods.

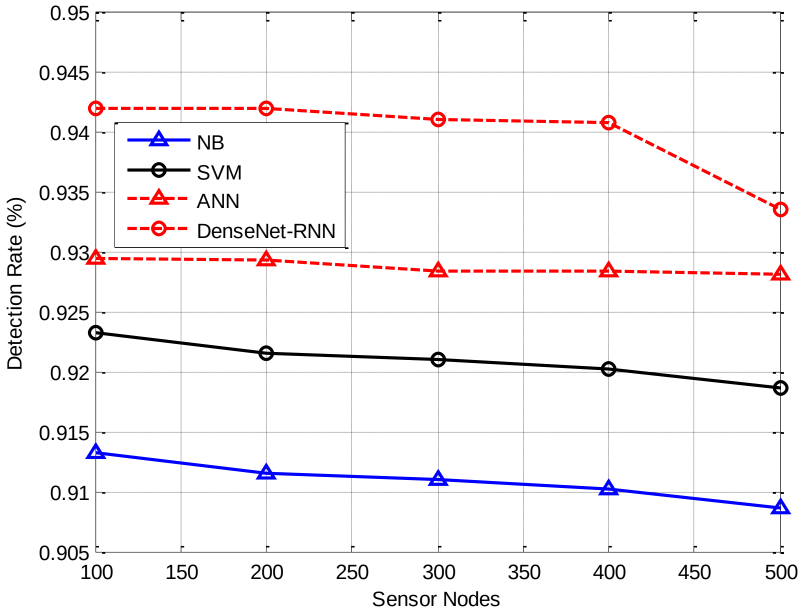

Figure 8: Detection Rate

Figure 8 shows the results of Detection Rate between DenseNet-RNN and existing ML models for the jamming attack mitigation. The results of simulation shows that the DenseNet-RNN is effective in detecting the jammers in WSN than other methods.

Statistical Analysis Measures

The most often used KPIs for evaluating the success of Intrusion Detection and Prevention Systems' in deep learning algorithms are accuracy, precision, recall and f-measure. The confusion Matrix, a two-dimensional matrix containing information on the Actual and Predicted classes, serves as the foundation for all assessment criteria.

- True-Positive (TP): Instances of data that the classifier properly classifies as an Attack
- False-Negative (FN): Instances of data that are mistakenly predicted as Normal
- False-Positive (FP): Instances of data that were identified mistakenly as an Attack.
- True-Negative (TN): Instances of data that were correctly classified as Normal

The confusion matrix's diagonal members reflect accurate predictions, whereas the nondiagonal components represent faulty assumptions made by a particular classifier.

The Table 1 shows the characteristics of the confusion matrix. In addition, some of the various assessment measures utilised in recent research included as follows:

	Predicted Class		
Actual Class		Attack	Normal
	Attack	True Positive	False Negative
	Normal	False Positive	True Negative

Table 2. Confusion Matrix

The simulation is conducted in terms of varying the attack size and the simulator is conducted to test the efficacy of the model in terms of accuracy, precision, recall and f-measure over different attacks and average of which are computed. The proposed method is further tested over various attacks that includes: fragmentation attacks, plashing and application layer attacks. These attacks come under the sub-categories of DoS attacks. Such evaluation is carried out in order to test the efficacy of the DenseNet-RNN under various DoS attacks. The results of the attack mitigation are given in Table.3.

Table.3. Other DoS Attack Detection

(a) Recall

Methods	Number of Nodes				
	100	200	300	400	500
Fragmentation Attacks					
NB	0.9820	0.9920	0.9820	0.9820	0.9920
SVM	0.9920	0.9920	0.9920	0.9719	0.9820
ANN	0.9920	0.9419	0.8116	0.7615	0.7214
Dense Net-RNN	**0.9442**	**0.934**	**0.9442**	**0.8528**	**0.998**
Plashing Attacks					
NB	0.9118	0.8317	0.7615	0.6914	0.5311
SVM	0.9920	0.9820	0.9820	0.9930	0.9920
ANN	0.9920	0.9820	0.9920	0.9569	0.9619
Dense Net-RNN	**0.9946**	**0.9946**	**0.9927**	**0.9634**	**0.9708**
Application layer attacks					
NB	0.9920	0.9920	0.9920	0.9940	0.9920
SVM	0.9820	0.9920	0.9920	0.9870	0.9920
ANN	0.9519	0.9619	0.8216	0.7545	0.7214
Dense Net-RNN	**0.9943**	**0.9942**	**0.9937**	**0.9964**	**0.9989**

(b) Precision

Methods	Number of Nodes				
	100	200	300	400	500
Fragmentation Attacks					
NB	0.9719	0.9419	0.9118	0.8216	0.8216
SVM	0.8918	0.8617	0.8517	0.8617	0.8617
ANN	0.9820	0.9619	0.9820	0.9719	0.9820
Dense Net-RNN	**0.9920**	**0.9920**	**0.9920**	**0.9820**	**0.9920**
Plashing Attacks					
NB	0.9719	0.9419	0.9118	0.8216	0.7816
SVM	0.8617	0.8818	0.8517	0.8617	0.8617
ANN	0.9619	0.9619	0.9619	0.9749	0.9820
Dense Net-RNN	**0.9920**	**0.9820**	**0.9920**	**0.9840**	**0.9845**
Application layer attacks					
NB	0.9619	0.9419	0.9218	0.8116	0.7816
SVM	0.8617	0.8517	0.8617	0.8367	0.8317
ANN	0.9619	0.9619	0.9619	0.9830	0.9820
Dense Net-RNN	**0.9920**	**0.9820**	**0.9920**	**0.9880**	**0.9920**

From the results of simulation, it is seen that the recall rates and precision rates of DenseNet-RNN under different DoS attacks are high in terms of detecting the attacks. The ANN model provides only a marginal difference with DenseNet-RNN. The other machine learning models like SVM and NB fails to detect the attacks and it is shown in terms of very less recall and precision rates.

5. Conclusions

In this paper, Intrusion Prevention System is developed that declines the rate of DoS attacks in WSN. The system uses DenseNet algorithm, which is trained with the training datasets to develop itself as a model for validating the attacks in WSN. The model trained detects the attack from the test dataset of DoS attack dataset. The study ran a series of simulations to see how well the sink performed and how much energy it used under a DoS attack. Despite the fact that network packets are not encrypted, the research shows that they can still be harmful and even bring the entire network to a halt, using up vital energy resources in the process. In order to avoid different sorts of DoS attacks, the security level can be adjusted according to the type of attack that is launched. According to the results of the simulation, decreasing the security level could help prevent or postpone a DoS attack in some circumstances.

Quality of Protection Modeling Language-supported multifaceted analysis made it possible to look at various devices' security metrics and gather results on multiple levels, starting with time and energy consumption, going through ecology and finance to quality of protection before concluding the study. The DenseNets concentrate on a single feature of an attack at a time, whereas a multilevel approach is being proposed, allowing for simultaneous examination of several aspects. In the future, this DoS attack model can be used to test different attack mitigation strategies and technologies.

References

[1] Chaitanya, D. K., & Ghosh, A. (2010). Analysis of denial-of-service attacks on wireless sensor networks using simulation. *Middlesex University*, 1-13.

[2] Pei, L., Li, C., Hou, R., Zhang, Y., & Ou, H. (2013). Computer simulation of denial of service attack in military information network using opnet. In *Proceedings of the 3rd International Conference on Multimedia Technology (ICMT'13)*.

[3] Doddapaneni, K., & Ghosh, A. (2011). Analysis of Denial-of-Service attacks on Wireless Sensor Networks using simulation. *IT Security for the Next Generation-European Cup 2011*.

[4] Bhatnagar, R., & Shankar, U. (2012). The proposal of hybrid intrusion detection for defence of sync flood attack in wireless sensor network. *International Journal of Computer Science and Engineering Survey*, *3*(2), 31.

[5] Son, J. H., Luo, H., & Seo, S. W. (2010). Denial of service attack-resistant flooding authentication in wireless sensor networks. *Computer Communications*, *33*(13), 1531-1542.

[6] Kumar, V. D., & Navaneethan, C. (2014). Protection against denial of service (dos) attacks in wireless sensor networks. *International Journal of Advanced Research in Computer Science & Technology*, *2*(1), 439-443.

[7] Eian, M., & Mjølsnes, S. F. (2011, October). The modeling and comparison of wireless network denial of service attacks. In *Proceedings of the 3rd ACM SOSP workshop on networking, systems, and applications on mobile handhelds* (pp. 1-6).

[8] Dini, G., & Tiloca, M. (2012, October). ASF: an attack simulation framework for wireless sensor networks. In *2012 IEEE 8th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)* (pp. 203-210). IEEE.

[9] Zhang, Y. Y., Li, X. Z., & Liu, Y. A. (2012). The detection and defence of DoS attack for wireless sensor network. *The journal of china universities of posts and telecommunications*, *19*, 52-56.

[10] Wazirali, R. and Ahmad, R., 2021. Machine Learning Approaches to Detect DoS and Their Effect on WSNs Lifetime. Computers, Materials & Continua, 70(3), pp.4922-4946.

[11] Wu, D., Jiang, Z., Xie, X., Wei, X., Yu, W. and Li, R., 2020. LSTM Learning With Bayesian and Gaussian Processing for Anomaly Detection in Industrial IoT. IEEE Transactions on Industrial Informatics, 16(8), pp.5244-5253.

[12] Mohd, N., Singh, A. and Bhadauria, H., 2019. A Novel SVM Based IDS for Distributed Denial of Sleep Strike in Wireless Sensor Networks. Wireless Personal Communications, 111(3), pp.1999-2022.

[13] Yadav A., Kumar A. (2022) Intrusion Detection and Prevention Using RNN in WSN. In: Smys S., Balas V.E., Palanisamy R. (eds) Inventive Computation and Information Technologies. Lecture Notes in Networks and Systems, vol 336.

[14] Borgiani, V., Moratori, P., Kazienko, J. F., Tubino, E. R., & Quincozes, S. E. (2020). Toward a Distributed Approach for Detection and Mitigation of Denial-of-Service Attacks Within Industrial Internet of Things. *IEEE Internet of Things Journal*, *8*(6), 4569-4578.

[15] Suryaprabha, E., & Kumar, N. S. (2020). Enhancement of security using optimized DoS (denial-of-service) detection algorithm for wireless sensor network. *Soft Computing*, *24*(14), 10681-10691.

[16] Islam, M. N. U., Fahmin, A., Hossain, M. S., & Atiquzzaman, M. (2021). Denial-of-Service Attacks on Wireless Sensor Network and Defense Techniques. *Wireless Personal Communications*, *116*(3), 1993-2021.

[17] E. Gelenbe and Y. Yin. Deep Learning with Dense Random Neural Networks. Proc. Int. Conf. on Man–Machine Interactions, Springer, 3–18,2017.