Intrusion Prevention Framework for WSN using Deep CNN

Pankaj R Chandre
Dr Parikshit N Mahalle
Dr Gitanjali R Shinde

Abstract: Today in the evers swifting world the life is changing towards ubiquitous computing and all human beings are releasing on the fly activity. In the view of this wireless sensor network is playing a key role in every use case. Due to the design issues like distributed nature, decentralized operations WSN is facing prominent security issues like attacks which includes Denial of Service (DoS), Black hole, Gray hole, Flooding and TDMA. This research puts forward a survey of state of the art. Furthermore this research also presents a full proof intrusion prevention framework based on deep learning and findings of the proposed system is also presented in this research with comparison of the state of the art. This paper also discusses the significance of the results and future outlook.

Keywords: Intrusion Detection and Prevention, WSN, CNN, Deep Learning

1. Introduction

The Wireless Sensor Network (WSN) is a group of sensor nodes spread over a geographical area that uses a wireless environment to transmit sensed data to each other. In a wireless sensor network (WSN), there is a communication in between sensors to sensors as well as with sensors to the base station that analyzes the collected data[1]. Now a day, in various fields there is a demand for wireless remote monitoring as well as control and that's why WSN become more and more popular. WSNs are widely used in areas like health monitoring, military applications, environment monitoring and many more[2]. But the basic aim of WSN is to collect meaningful data from the environment. Basically, in intrusion detection we can monitors the network traffic as well as analyzes the data to check whether there is any malicious activity[3]. The basic aim of such type of system is to detect and defend the network from unauthorized users[4]. Basically, in unauthorized users we can consider active attackers and the examples of active attackers are like Denial of Service attack, flooding, blackhole attack[5][6] and many more. The main aim of an intrusion prevention system is to identify the malicious activity, and after that either detect and allow or prevent that malicious activity.Basically, in the field of intrusion detection and prevention, few number of research studies have investigated deep learning, but none of these have successfully utilized the full power of deep learning methods[7][8].Now a day, deep learning are widely used in many areas like cyber security, speech recognition, machine translation and many more[7][9].By using Deep learning methods, we can improve the effectiveness as well as accuracy rate of intrusion detection and prevention in WSN[10][11]. In deep learning, convolutional neural network (CNN) is the mostly used method[12].

2. Related Work

Similar work in the field of intrusion detection and prevention system using deep learning are presented and discussed in this section.

D Mehetre et al have proposed a method for intrusion detection and intrusion prevention in WSN[8]. In this work, author proposed a trustable and secure scheme by using two stage mechanisms. Basically proposed work is able to identify trusted path for the purpose of transmission of data packets. The proposed work is able to prevent selective forwarding and black hole in WSN.

Jorge Granjal et al have proposed a framework for the purpose of intrusion detection and prevention[13]. In this authors have used anomaly based techniques to prevention intrusion like denial of service attack. In this work authors have used Support Vector Machine (SVM) as a classifier and they achieved better results. Again in this work, authors have achieved 93% accuracy if the intrusion is well known.

Oke et al have proposed a two layers trust based IPS for WSN[14]. The proposed system is able to detect intrusions in the network. In proposed system, authors have considered multiple scenarios by selecting different set of weights. To achieve better accuracy authors have tried multiple combinations of sets. The average accuracy of proposed system is 96%.

Clifford Green et al have implemented a deep learning model for intrusion detection like Denail of Service attack[15]. In this authors have used DNN and RNN. In this work for implementation purpose authors have used with NSL KDD dataset and compared there results with logistic regression techniques. An accuracy of proposed algorithm is 79.20%.

Sinan Calisur et al have proposed a model for intrusion detection and intrusion prevention[16]. In this work authors have used machine learning and deep learning techniques to detect Denial of Service attack. For implementation purpose, authors have used NSL KDD dataset with Random Forest, Support Vector Machine, Convolutional Neural Network any many more techniques. An accuracy of detecting Denial of Service attack is 96%.

Peilun Wu and Hui Guo have proposed a deep learning model for intrusion detection[17]. In this work authors have used convolutional neural network (CNN) and recurrent neural network (RNN) model with NSL KDD Cup99 dataset. The CNN and RNN model is able to learn input traffic data and after that the features are extracted. On the basis of experimentation, the proposed model gives better accuracy with low rate of false positive.

Navaporn Chockwanich, Vasaka Visoottiviseth have proposed an intrusion detection model using deep learning[18]. In this work authors have used supervised learning like convolutional neural network and recurrent neural network with TensorFlow. The proposed model is able to detect Denial of Service attack just by considering the header information of packet. For implementation purpose, authors have pcap files and then compared their results with Snort IDS. The proposed model gives better accuracy as compare to the existing one.

Farrukh Aslam Khan et al have proposed a two stage deep learning model for intrusion detection[19]. The proposed model is able to learn useful features from large amount of labeled data and then performs classification. For implementation purpose, authors have used KDD99 dataset and the accuracy of proposed model is 89.13%.

3. Proposed Methodology

3.1. Framework

In WSN scenario, there are different sensor nodes sending some or other parameters or there are individualsensor network deployed for specific purpose. These sensor networks can be used for different use cases like indoor/outdoor. When these sensor networks can use by one of the existing access network technologies based on the use case. These access network technologies include 2G/3G/4G, WiFi, LTE and WiMax. When these WSNs are connected to Internet they can post data to the cloud or Plug and Play devices can also download data from cloud. Looking at this entire ubiquitous scenario, intrusion is possible between application layer and access network layer. So to handle these intrusion, intrusion prevention layer plays an important role which is the key contribution of this research. To handle these intrusions, deep learning classifier like Convolutional Neural Network is better. The key layer in the framework is intrusion prevention layer. The main functionality of this layer is to track the intrusion which is taking place in between mainly application layer and sensor layer. The detection of intrusion is mainly based on the analysis of packet header and prevention is based on analysis of payload irrespective of the underline computer network. Essentially in the context of wireless network the prevention is more crucial task due to the factors like dynamic topology, distributed network and decentralized nature. However in the scope of this paper, these network parameters are assumed by default. To propose mitigation strategies against any attack it is very important to perform threat analysis and attack modeling of underline networks. In the sequel, the first functional block of this layer is to perform behavioral modeling of threats and respective underline attacks. After this the next functional block is to perform detection of intrusion based on the header analysis. In order to enable proactive functioning of this layer learning techniques plays a very important role. In the view of this, the next task is to build a machine learning based model to initiate further operations adaptively. In the next step the model is built for the payload dataset using Convolutional Neural Network with the help of three hidden layer. The appropriate separation of training and testing of dataset is used for all the experimentation. The outcome of this model is the time aware rules to identify the appropriate attack which is the main outcome of deep learning approach. Finally based on this time aware rules attack mapping is done which is the main outcome of this layer in the proposed framework. The proposed intrusion prevention framework is shown in Figure 1.

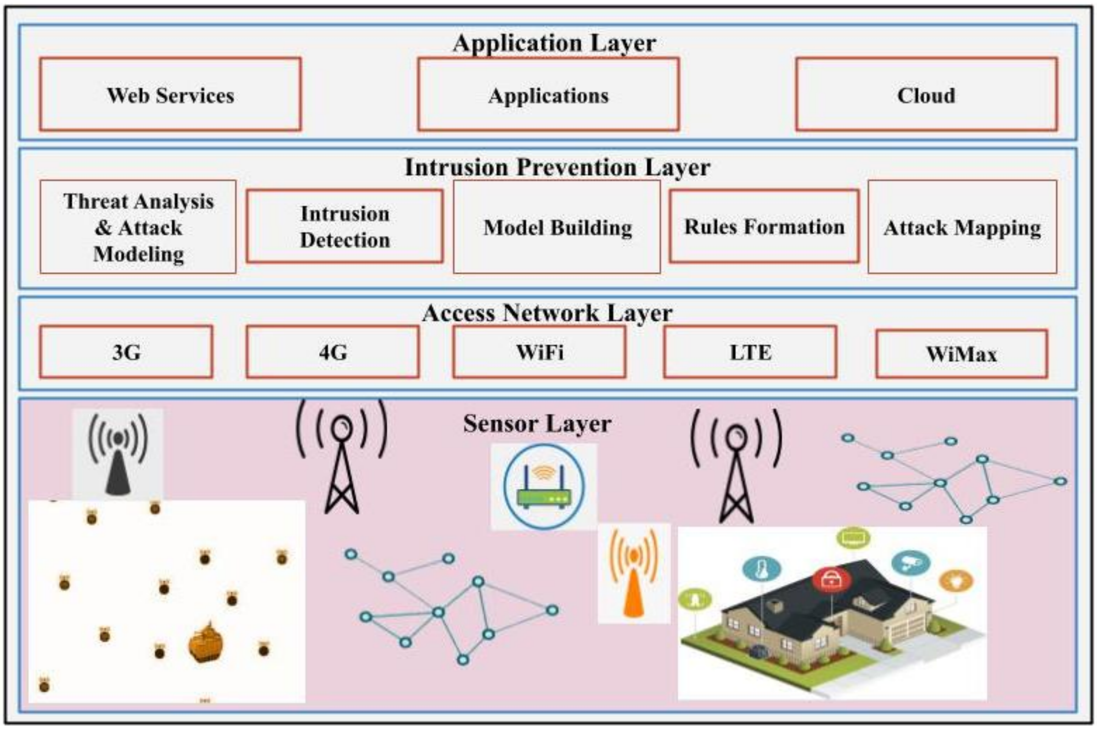

Figure 1. Intrusion prevention framework

3.2. Mathematical Model

An intrusion prevention system (IPS) using deep packet inspection for WSN is represented as:
IPS= {Tr,Pr,Fr,Wm,Iv,Hv,O}
Tr- Training dataset selection
Pr- Preprocessing on the training dataset
Fr- Select training dataset with features
Wm- Weight matrix
Iv- Offset vector of input unit
Hv- Offset vector of hidden unit
O- Output as Normal, Black hole, Gray hole, Flooding

Preprocessing:

In this step, the training data (TR) is normalized to be equipped for processing by using following formula:

$$TR_{norm} = \{\frac{TR-\mu_T}{\sigma_T}, \sigma_T \neq 0 \; and \; TR - \; \mu_T, \sigma_T = 0 \qquad (1)$$

Where,

$$TR = \{x_{i,j} | i = 1,2, \ldots, m \; and \; j = 1,2,3, \ldots, n\}$$
$$\mu_T = \{\mu_j | j = 1,2,3, \ldots, n\}$$
$$\sigma_T = \{\sigma_j | j = 1,2,3, \ldots, n\}$$

TR is m samples with n column attributes; x_{ij} is the jth column attribute in ith sample, μ_T and μ_T are 1*nmatrix which are the training data mean and standard deviation respectively for each of the n attributes. The test dataset (TE) which is used to measure prevention accuracy is normalized using the same μ_T and μ_T as follows:

$$TE_{norm} = \frac{(TE-\mu_T)}{\sigma_T}, \sigma_T \neq 0 \; and \; TE - \mu_T, \sigma_T = 0 \qquad (2)$$

Convolution:
By using this layer, we can extract the features from an input data. Basically, it a mathematical operation which uses two inputs like filter and data matrix[20]. We can consider, an data matrix with dimension (h x w x d),a filter (Fh x Fw x D) and output with dimension (h –Fh + 1) X (w –Fw + 1) x 1.

Pooling:
Basically, in CNN pooling payer is used to speed up the calculations as well as to reduce the size of tensor. In this layer simply we have to divide our data into multiple parts and after that we can perform operations on those parts[21]. We can perform operations like Min Pooling, Average Pooling and Max Pooling. Again with this, two hyper parameters are available like stride and filter size.

Activation function:
Activation functions are very important for CNN; it is used to to convert a input signal into output signal[22]. And an output signal is used as an input to next layer.In this we have used sigmoid activation function of form f(x) = 1 / 1 + exp(-x)

Fully Connected Layer:
And, lastly the output of pooling layer is used as an input to fully connected layer[11]. By using this layer, every node from first layer is connected to every node in second layer.
The main contributions of this proposed research are:

- Survey on intrusion prevention using deep learning
- Intrusion prevention framework design using deep learning
- Findings of proposed system are compared and discussed with existing system
- Discussion on why the proposed system is better as compare to existing system

4. Results and Discussions

In this section, the findings of proposed system are compared with the existing system in terms of intrusion prevention. Why the proposed system is better than the existing system are presented with the help of comparison. The proposed system is implemented by using a WSN-DS dataset[23] and a python as a programming tool and a Tensor Flow on a system equipped with 128GB RAM, 1TB system SSD, 2TB data SSD, Intel Xeon-W 2145 8 Core and Titan V GPU's. The overall accuracy of the proposed system is 97%. The proposed system is compared with state of art and it gives better accuracy in terms of intrusion prevention. The confusion matrix for proposed system is shown in Table 1.

Table 1. Confusion matrix

	Precision	Recall	*F1 Score*
Normal	0.99	0.99	0.99
Blackhole	0.94	0.90	0.92
Grayhole	0.89	0.81	0.85
Flooding	0.73	0.50	0.59
TDMA	0.63	0.93	0.75
Accuracy	0.97	0.97	0.97

Figure 2 shows the comparison of proposed system with existing work. In [13], authors have proposed a framework for intrusion detection and prevention system using support vector classifier to prevent denial of service attack with accuracy 93% and it is denoted as bar(A).
In [14], authors have proposed a two layer trust based intrusion prevention system for WSN. In this work, authors have considered multiple scenarios by selecting different set of weights and the accuracy of system is 96% which is denoted as bar(B).
In [19], authors have proposed a two stage deep learning model for intrusion detection. The proposed model is able to learn useful features from large amount of data and the accuracy of model is 89.13% which is denoted as bar(C).
In [15], authors implemented a deep learning model for intrusion detection like denial of service attack and the accuracy of model is 79.20% which is denoted as bar(D).
The accuracy of our proposed model is 97% which is denoted as bar(E) and on the basis of comparison we can say the proposed system is better as compare to the existing models. The proposed system is tested many times with variable data size and performance of the system is not getting affected with the variation in data. That's

why the Convolutional Neural Network algorithms are better to detection and prevent intrusion for wireless sensor networks.

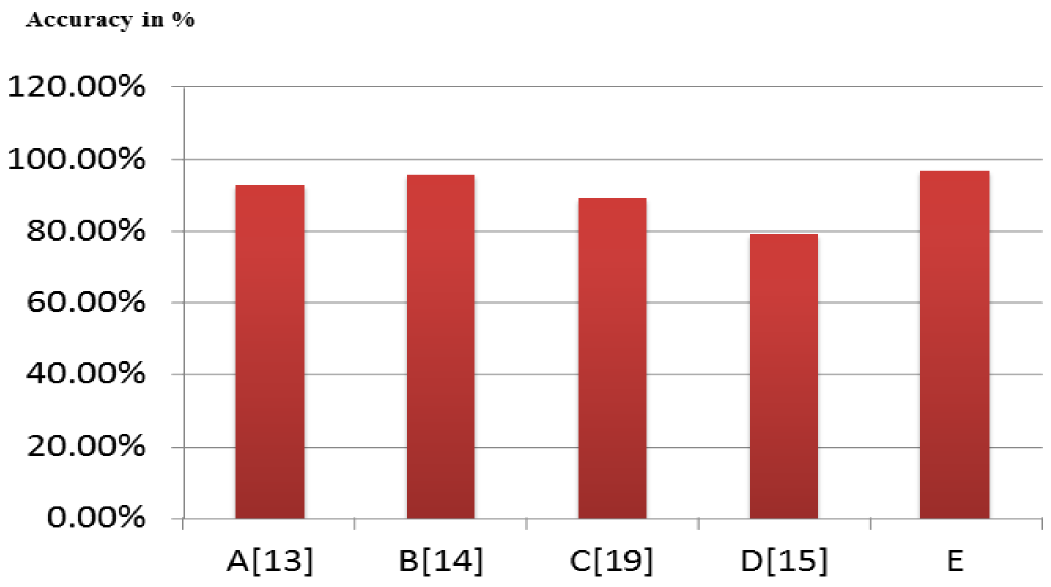

Figure 2. Accuracy comparison with existing system

5. Conclusions and Future Scope

In this work, intrusion prevention framework based on deep learning is proposed. The CNN algorithm is used in this work to prevent the various intrusions. Looking at the possible attacks in between application layer and the access network layer, the proposed framework is able to handle intrusion like black hole, gray hole, flooding and TDMA. The results of proposed system are compared with the existing mechanisms and the comparison results shows that proposed system gives better performance with an accuracy of 97%. As compared to existing system, there is an improvement of 1% in terms of intrusion detection and prevention for WSN. The future outlook of the work is to apply the same model on real time data sets.

References

1. Ajeetha, G., & Madhu Priya, G. (2019). Machine Learning Based DDoS Attack Detection. 2019 Innovations in Power and Advanced Computing Technologies, I-PACT 2019, 234–237. https://doi.org/10.1109/i-PACT44901.2019.8959961
2. Almomani, I., Al-Kasasbeh, B., & Al-Akhras, M. (2016). WSN-DS: A Dataset for Intrusion Detection Systems in Wireless Sensor Networks. Journal of Sensors, 2016(January). https://doi.org/10.1155/2016/4731953
3. Almomani, I., & Alenezi, M. (2018). Efficient Denial of Service Attacks Detection in Wireless Sensor Networks. Journal of Information Science and Engineering, 34(4), 977–1000. https://doi.org/10.6688/JISE.201807_34(4).0011
4. Calisir, S., Atay, R., Pehlivanoglu, M. K., & Duru, N. (2019). Intrusion Detection Using Machine Learning and Deep Learning Techniques. UBMK 2019 - Proceedings, 4th International Conference on Computer Science and Engineering, 656–660. https://doi.org/10.1109/UBMK.2019.8906997
5. Chandre, P. R., Mahalle, P. N., & Shinde, G. R. (2018). Machine Learning Based Novel Approach for Intrusion Detection and Prevention System: A Tool Based Verification. 2018 IEEE Global Conference on Wireless Computing and Networking (GCWCN), 135–140. https://doi.org/10.1109/GCWCN.2018.8668618
6. Chockwanich, N., & Visoottiviseth, V. (2019). Intrusion Detection by Deep Learning with TensorFlow. International Conference on Advanced Communication Technology, ICACT, 2019–Febru, 654–659. https://doi.org/10.23919/ICACT.2019.8701969
7. Das, S. K., Samanta, S., Dey, N., & Kumar, R. (2019). Design Frameworks for Wireless Networks (Vol. 82). http://dx.doi.org/10.1007/978-981-13-9574-1_12%0Ahttp://link.springer.com/10.1007/978-981-13-9574-1

8. Granjal, J., Silva, J. M., & Lourenço, N. (2018). Intrusion detection and prevention in CoAP wireless sensor networks using anomaly detection. Sensors (Switzerland), 18(8). https://doi.org/10.3390/s18082445
9. Gulla, K. K., Viswanath, P., Veluru, S. B., & Kumar, R. R. (2019). Machine learning based intrusion detection techniques. Handbook of Computer Networks and Cyber Security: Principles and Paradigms, Icoei, 873–888. https://doi.org/10.1007/978-3-030-22277-2_35
10. Home, S., Using, S., & Systems, P. (2019). Detection and Prevention Systems.Jyothsna, V., V. Rama Prasad, V., & Munivara Prasad, K. (2011). A Review of Anomaly based Intrusion Detection Systems. International Journal of Computer Applications, 28(7), 26–35. https://doi.org/10.5120/3399-4730
11. Khan, F. A., Gumaei, A., Derhab, A., & Hussain, A. (2019). TSDL: A Two-Stage Deep Learning Model for Efficient Network Intrusion Detection. IEEE Access, 7(c), 30373–30385. https://doi.org/10.1109/ACCESS.2019.2899721
12. Lee, B., Amaresh, S., Green, C., & Engels, D. (2018). Comparative Study of Deep Learning Models for Network Intrusion Detection. SMU Data Science Review, 1(1), 8.
13. Mehetre, D. C., Roslin, S. E., & Wagh, S. J. (2019). Detection and prevention of black hole and selective forwarding attack in clustered WSN with Active Trust. Cluster Computing, 22(S1), 1313–1328. https://doi.org/10.1007/s10586-017-1622-9
14. Mohammadpour, L., Ling, T. C., Liew, C. S., & Chong, C. Y. (2018). A Convolutional Neural Network for Network Intrusion Detection System. Proceedings of the Asia-Pacific Advanced Network, 46(0), 50–55.
15. Oke, J. T., Agajo, J., Nuhu, B. K., Kolo, J. G., & Ajao, L. A. (2018). Two Layers Trust-Based Intrusion Prevention System for Wireless Sensor Networks. Advances in Electrical and Telecommunication Engineering, 1(1), 23–29.
16. Osken, S., Yildirim, E. N., Karatas, G., & Cuhaci, L. (2019). Intrusion detection systems with deep learning: A systematic mapping study. 2019 Scientific Meeting on Electrical-Electronics and Biomedical Engineering and Computer Science, EBBT 2019, 1–4. https://doi.org/10.1109/EBBT.2019.8742081
17. Peng, W., Kong, X., Peng, G., Li, X., & Wang, Z. (2019). Network intrusion detection based on deep learning. Proceedings - 2019 International Conference on Communications, Information System, and Computer Engineering, CISCE 2019, 431–435. https://doi.org/10.1109/CISCE.2019.00102
18. Phadke, A., Kulkarni, M., Bhawalkar, P., & Bhattad, R. (2019). A review of machine learning methodologies for network intrusion detection. Proceedings of the 3rd International Conference on Computing Methodologies and Communication, ICCMC 2019, Iccmc, 272–275. https://doi.org/10.1109/ICCMC.2019.8819748
19. Taher, K. A. (2019). Network Intrusion Detection using Supervised Machine Learning Technique with Feature Selection. 2019 International Conference on Robotics,Electrical and Signal Processing Techniques (ICREST), 643–646.
20. Wu, P., & Guo, H. (2019). LuNet: A Deep Neural Network for Network Intrusion Detection. 2019 IEEE Symposium Series on Computational Intelligence, SSCI 2019, 617–624. https://doi.org/10.1109/SSCI44817.2019.9003126
21. Yang, H., Qin, G., & Ye, L. (2019). Combined Wireless Network Intrusion Detection Model Based on Deep Learning. IEEE Access, 7, 82624–82632. https://doi.org/10.1109/ACCESS.2019.2923814
22. Zhang, R., & Xiao, X. (2019). Intrusion detection in wireless sensor networks with an improved NSA based on space division. Journal of Sensors, 2019(1). https://doi.org/10.1155/2019/5451263