Deep learning intrusion detection system for mobile ad hoc networks against flooding attacks

Oussama Sbai, Mohamed Elboukhari
Department of Applied Engineering, ESTO (Higher School of Technology) Mohammed 1st University, Oujda, Morocco

Article Info

Article history:

Received Apr 16, 2021
Revised May 21, 2022
Accepted Jun 2, 2022

Keywords:

CICDDoS2019 dataset
Data flooding attack
Deep learning
Deep neural network
Intrusion detection system
MANETs
SYN flooding attack
UDP flooding attack

ABSTRACT

Mobile ad hoc networks (MANETs) are infrastructure-less, dynamic wireless networks and self-configuring, in which the nodes are resource constrained. With the exponential evolution of the paradigm of smart homes, smart cities, smart logistics, internet of things (IoT) and internet of vehicle (IoV), MANETs and their networks family, such as flying ad-hoc networks (FANETs), vehicular ad-hoc networks (VANETs), and wireless sensor network (WSN), are the backbone of the whole networks. Because of their multitude use, MANETs are vulnerable to various attacks, so intrusion detection systems (IDS) are used in MANETs to keep an eye on activities in order to spot any intrusions into networks. In this paper, we propose a knowledge-based intrusion detection system (KBIDS) to secure MANETs from two classes of distributed denial of service (DDoS) attacks, which are UDP/data and SYN flooding attacks. We use the approach of deep learning exactly deep neural network (DNN) with CICDDoS2019 dataset. Simulation results obtained show that the proposed architecture model can attain very interesting and encouraging performance and results (Accuracy, Precision, Recall and F1-score).

Corresponding Author:

Oussama Sbai
Department of Applied Engineering, ESTO (Higher School of Technology) Mohammed 1st University
Oujda, Morocco
Email: o.sbai@ump.ac.ma

1. INTRODUCTION

A mobile ad hoc network (MANET) is a self-organizing group, self-connected of mobile nodes without using central administration and fixed infrastructure. When a node wants to create a connection with another node outside of its communication range, its node's neighbors collaborate with it and transmit the messages. Therefore, the nodes of MANETs behave as a router as well as a host. The network's topology is temporary and constantly changing. Added to that, nodes can leave the network and new ones can join it. MANETs have a number of advantages over classical networks, in that they can straightforwardly be implement and disassemble, as well as the flexibility provided by the fact that the nodes are not attached.

MANET's applications are in continuous development and cover a variety of areas, like vehicular ad-hoc network (VANET) [1] in smart road traffic [2], smart cities and smart home, in general smart environment [3]. Furthermore, flay ad hoc network (FANET) in smart air traffic [4]. Besides being operable as a stand-alone network, ad hoc networks can also be attached to the Internet [5], such as the paradigm of internet of things (IoT) [6] and internet of vehicle (IoV) [7].

Intrusion detection system (IDS) is the mechanism used by the network's nodes for monitoring and analyzing the network traffics, for which of these last represent a breach of security policy and standards, thus report any illegal or malicious activity [8]. Based on the detection methodologies used, the IDS are divided into four categories [9], [10]:

- ABID: Anomaly-based or behavior-based intrusion detection.
- KBID: Knowledge-based, also known as Misuse or Signature intrusion detection.
- SBID: Specification-based intrusion detection.
- Hybrid or compound IDS, it is a combination and fusion of the different precedent detection techniques.

This work represents a continuation of our previous ones, where we studied the attacks in MANETs [11], and an extension and improvement of [12] and [13]. In this paper, we present a deep neural network IDS (DNN-IDS) for MANETs against both Distributed UDP/data and SYN flooding attacks. The presented models exhibit good results, according to the result of our experiments.

The paper's organization is: section 2 presents some related works. The description of the proposed work is presented in section 3, with definition of the context of this work, the grid search to develop an adequate DNN model, the utilized dataset, plus the selected features. Section 4 discusses the experimental results obtained. At the end, we closed this work by a conclusion.

2. RELATED WORKS

This section is considerate to present a works, which they have employed deep learning approach in IDS for MANETs and they derivate like VANETs. In the paper [14], the authors propose a protection mechanism based on the artificial neural network algorithm together with the swarm-based artificial bee colony optimization technique, against blackhole and grayhole attacks for MANETs using Ad hoc On-demand Distance Vector (AODV) protocol. In [15], Feng *et al.* suggest an IDS installed in plug and play device to detect denial of service (DoS), XSS and SQL attacks for ad hoc network on using deep learning model. The author uses KDD99 dataset plus the XSS and SQL attack sample collected from waf log. In the work [16], Zeng *et al.* present a deep learning IDS to detect blackhole, wormhole, sybil and distributed denial of service (DDoS) attacks in VANETs. In experimental phase, they use ISCX 2012 IDS dataset [17] and simulated dataset on using ns-3 simulator [18]. Sowah *et al.* [19] advance an artificial neural network IDS to detect the man-in-the-middle (MITM) attack and identify the malicious nodes for MANETs using AODV protocol. The paper use dataset generated by ns-2 simulator to describe the performance of developed IDS. In the work [20], Alheeti and McDonald-Maier develop an intelligent hybrid IDS by combining knowledge and anomaly detection methods for VANETs. The IDS is based on proportional overlapping scores method (POS), multilayer perceptron (MLP) and fuzzy system to detect DoS attack. The authors use the Kyoto dataset for the performance tests. In this paper [21], Vimala *et al.* combine neural network algorithm, support vector machine and fuzzy system in their proposed IDS for MANETs. For the test phase, the authors use the KDD99 dataset. In the anterior works [12] and [13], we proposed two IDSs for MANETs, one to detect UDP flooding attack and the other to detect SYN flooding attack, on using DNN. The CICDDoS2019 dataset is used to test the proposed IDS.

3. WORK DESCRIPTION

3.1. Context of proposed work

UDP or data flooding attack as her name defines it when the attackers nodes inject in MANETs a great volume of nugatory UDP packets, is also a type of DDoS attacks. As a result, the unnecessary packets overload the network and decrease its bandwidth. Besides, consume the battery of intermediate nodes [11]. In the previous works [22] and [12], where we used the ns-3 platform [23] to study the MANET's reaction with AODV [24] and OLSR [25] protocols when a data flooding malicious nodes exist in network, the results showed that the network's normalized routing load (NRL) increases and the network's packet delivery ration PDR decreases by a significant values. Another type of DDoS and flooding attack that MANETs suffer from is SYN flooding attack, this attack works by making use of the TCP connection's three-way handshake process [11].

Among the solutions to detect these types of attacks, there is the method of Knowledge-based intrusion detection systems (KBIDS). The Figure 1 describe the architecture of KBIDS: the IDS save a knowledge or an internal database that contains signatures or patterns of already known threats and looks if any user's activity matches with stored patterns/signatures, then an alarm will trigger. In knowledge-based intrusion detection (KBID) mechanism, an event is proclaimed as non-intrusive or acceptable, if is not formally acknowledged as a threat based on existing internal database. However, if an event that has reduced network performance is detected as an unknown attack because it does not match the saving rules, the IDS add a new rule to the existing knowledge database.

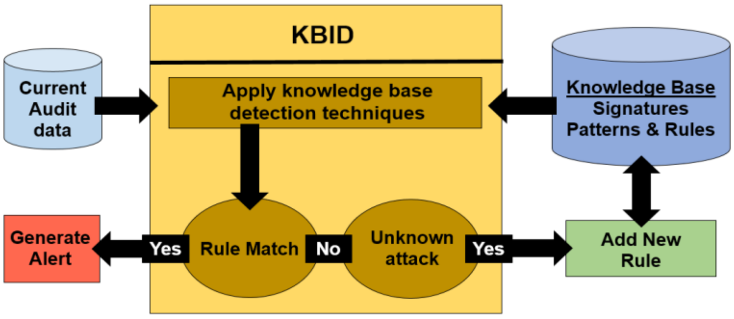
KBID
Current Audit data
Apply knowledge base detection techniques
Knowledge Base Signatures Patterns & Rules
Generate Alert
Yes
Rule Match
No
Unknown attack
Yes
Add New Rule

Figure 1. Knowledge-based intrusion detection (KBID) [26]

3.2. CICDDoS2019 dataset

The CICDDoS2019 Dataset has been defined in [27], has 80 network traffic features collected from principal component analysis of proteomics (PCAP) files by the CICFlowMeter software, which is freely available on the Canadian Institute for Cybersecurity website [28]. The dataset contains 12 types of DDoS attack, each attack is delivered in his specific file. In our case, we use file of UDP and SYN attack. In the precedent work [11], we studied the existed attacks that suffer from MANETs, and we find UDP and SYN flooding attack are a part of them. For the other attacks presented in this dataset are not considered for MANETs, due to use applications and the nature of all system MANETs.

3.3. Proposed methodology

To insure the scalability of our proposed IDS, we use a Standalone-based scheme in MANETs and nodes share detection results with their neighbors, with a privacy process [29] to secure the network transactions between them. Because we are concentrating on intrusion detection, the intricacies of these processes are outside the scope of this paper. Table 1 presents the grid search of network structure and hyper-parameters used to develop an optimal neural network topology. In our proposed solution for detecting UDP and SYN flooding attacks in MANETs, we have selected 11 features to use in the proposed DNN model, where Table 2 presents their definitions. The step involved in the DNN-IDS is shown in Figure 2.

Table 1. Hyper-parameters configured for grid search

Hyper-parameter	Values
Number of layers	3; 4
Number of nodes	37-75
Weight initialization	random_normal; he_uniform
Optimization	rmspop
Loss function	categorical_crossentropy
Learning rate	0.01; 0.001; 0.0001

Table 2. Features used in the proposed DNN model

Feature	Description
ACK Flag Count	Number of packets with ACK
Init Win bytes forward	The total number of bytes sent in initial window in the forward direction
min seg size forward	Minimum segment size observed in the forward direction
Fwd IAT Total	Packets flow inter arrival total time.
Flow Duration	Length of connection in seconds
Destination port	Port receiving packets
Protocol	Type of the protocol used
Fwd IAT Min	Packets flow inter arrival time Min.
Fwd IAT Max	Packets flow inter arrival time Max.
Packet Length Std	Standard deviation of the packet length
Fwd Packet Length Std	Standard deviation of a packet in the forward direction

3.4. Statistical measures

To select the best and adequate DNN model, we use accuracy, recall, F1-score, and precision as performance metrics. In the mathematical equation shown (1)-(4), the true positive (TP) and the true negative (TN) define the number of samples that were correctly classified as Benign and Attack class respectively.

The false positive (FP) and the false negative (FN) are the number of Benign and Attack samples respectively, that have been incorrectly identified as Attack samples.

$$\text{Accuracy} = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{TN} + \text{FP} + \text{FN}} \tag{1}$$

$$\text{Precision} = \frac{\text{TP}}{\text{TP}+\text{FP}} \tag{2}$$

$$\text{Recall} = \frac{\text{TP}}{\text{TP}+\text{FN}} \tag{3}$$

$$\text{F1} - \text{Score} = 2 \times \frac{\text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}} \tag{4}$$

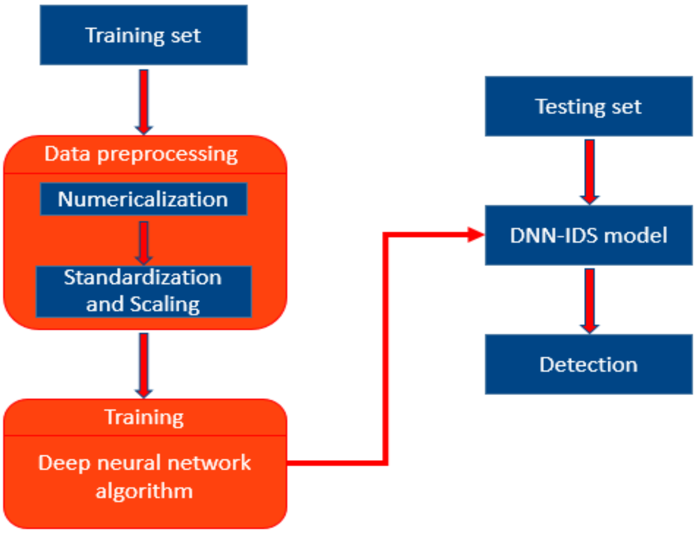

Figure 2. Block diagram of proposed DNN-IDS

4. EXPERIMENTAL RESULTS AND DISCUSSION

In our experiment, we combined the different possibilities of hyper-parameters values presented in Table 1, in order to obtain the best optimal results and suitable for the case of MANETs, and we constructed the training set and testing set from CICDDoS2019 dataset according to the paper. Table 3 describe in detail the training and testing sets. In Table 4, we present the different configuration of DNN architecture, who gave us the results presented in Figures 3 to 7. We remark that we executed the DNN a maximum of 4 layers and between 37 and 75 of total hidden nodes. This choice is made by taking into consideration the weak points of MANET's nodes (power limitation, limiting memory and calculation consumption); The learning rate parameter is fixed in 0.001 value, because in the test phase other value do not give us a good result. Briefly, in this table, we present the configuration of the promoting DNN models.

Table 3. Different classifications in the training and testing sets

Class	Number of training samples	Number of testing samples
Benign	37 947	3 526
SYN	4284751	1582289
UDP	3134645	3754680

The experimental results are presented in Figures 3 to 7. In terms of accuracy as shown in Figure 3, the Model 3 by 99.94% outperforms Model 5, Model 7, and Model 8 by 0.19%, 1.34% and 0.02% respectively. For the precision as shown in Figure 4, the Model 8 by 99% outperforms Model 3 by 1% and other models by 32%. Recall as shown in Figure 5 of the Model 11 by 97% outperforms Model 6 and Model 2 by 1%, Model 2 and Model 4 by 2%, Model 7 and Model 9 by 3%, Model 12 by 5%, Model 1 and Model

10 by 7%, Model 5 by 16%, Model 3 by 17% and Model 8 by 29%. F1-score as shown in Figure 7 of the Model 3 by 84% outperforms Model 5 by 11%, Model 8 by 14%, Model 7 by 15%, Model 11 by 16%, Model 9 by 17%, Model 2, Model 4, Model 6, and Model 12 by 18%, and Model 1 by 20%. In terms of Loss as shown in Figure 6, we remark the best performance are those of Model 3, Model 5, and Model 8. The Model 8 by 1.2% outperforms Model 5 (Loss = 1.3%) by 0.1%, Model 3 (Loss = 2.6%) by 1.4%.

On analyzing the confusion matrix of the Model 3 presented in Table 5, and by making a comparison of all the parameters, we find the Model 3 (yellow row in Table 4) has the best results: with a lead of +0.19% of the Model 8 which is the most efficient of the other models in term of accuracy. A difference of 1% of the best result (Model 8) in term of precision, and with a lead of +0.11% of the Model 5 which is the most efficient of the other models in term of F1-score. For the Loss scalar, there is a difference of 1.4% of the best results offered by Model 8. Taking into consideration the use cases of the MANETs, we choose the model who has the minimum number of layers and hidden nodes, because more nodes imply power and calculation consumption.

Table 4. DNN models

	Layers	Nodes	Weight initialization	Learning rate
Model 1	3	37	random_normal	0.001
Model 2	3	39	random_normal	0.001
Model 3	**3**	**39**	**he_uniform**	**0.001**
Model 4	3	40	random_normal	0.001
Model 5	3	42	he_uniform	0.001
Model 6	3	48	he_uniform	0.001
Model 7	3	48	random_normal	0.001
Model 8	3	53	he_uniform	0.001
Model 9	3	55	he_uniform	0.001
Model 10	4	52	random_normal	0.001
Model 11	4	71	random_normal	0.001
Model 12	4	75	random_normal	0.001

Table 5. Confusion matrix of Model 3

	Benign	SYN	UDP
Benign	1304	408	1814
SYN	88	3754503	89
UDP	1	553	1581735

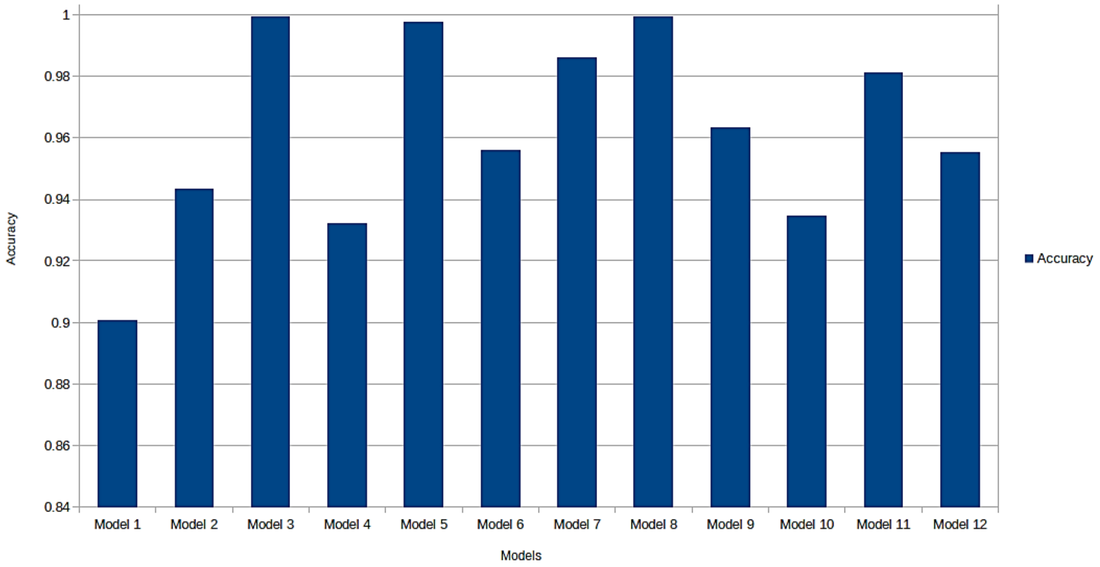

Figure 3. Accuracy results of DNN models

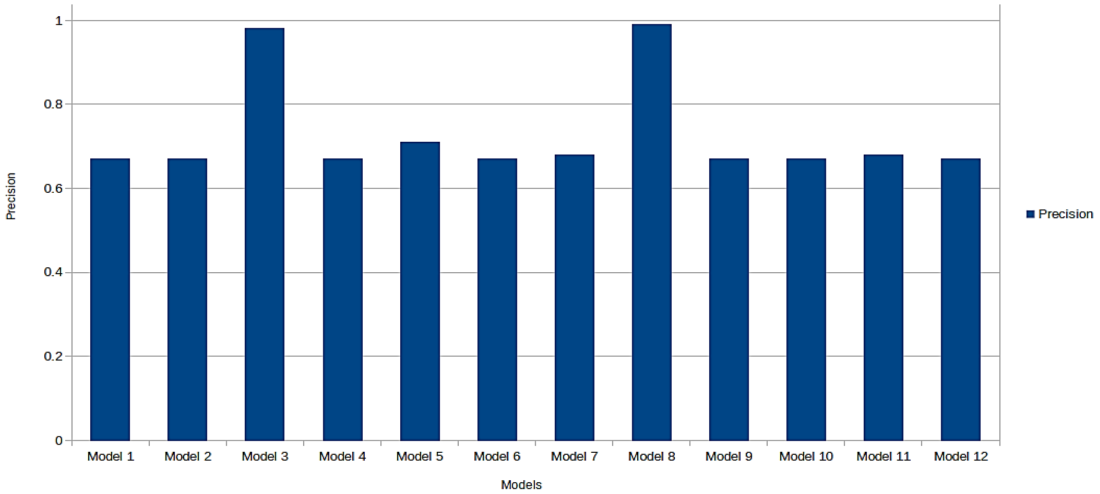

Figure 4. Precision results of DNN models

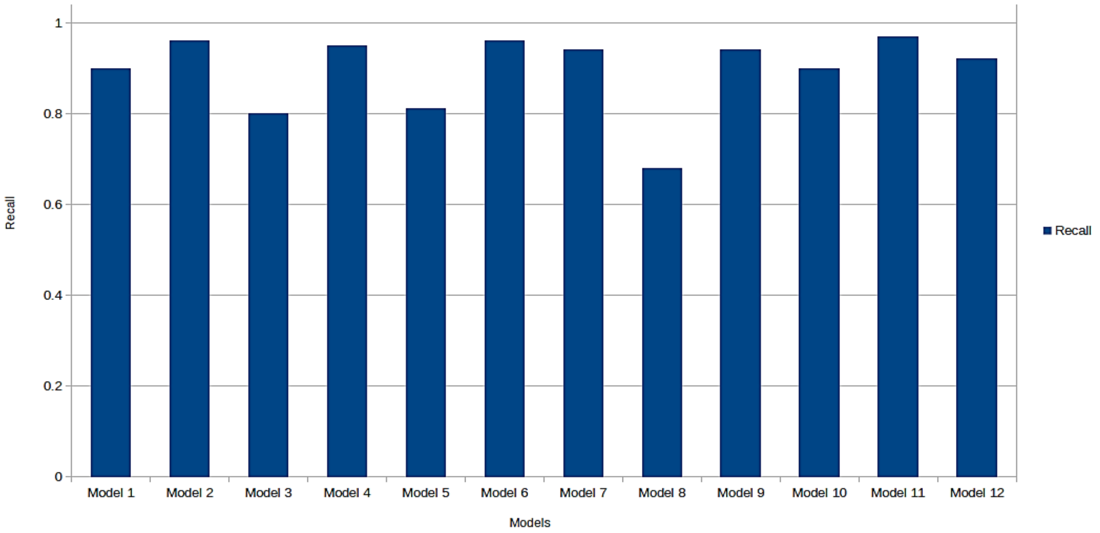

Figure 5. Recall results of DNN models

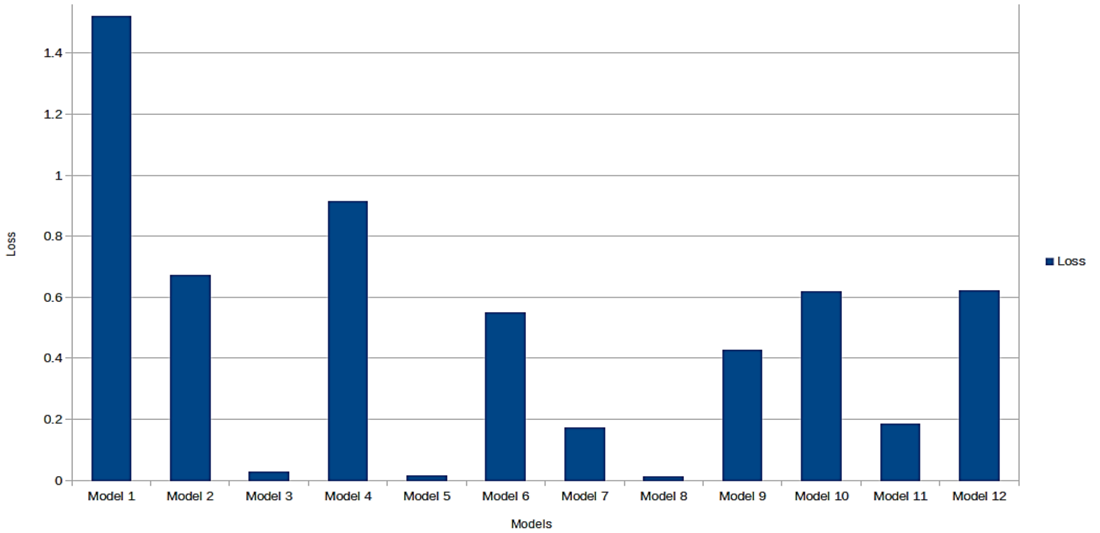

Figure 6. Loss results of DNN models

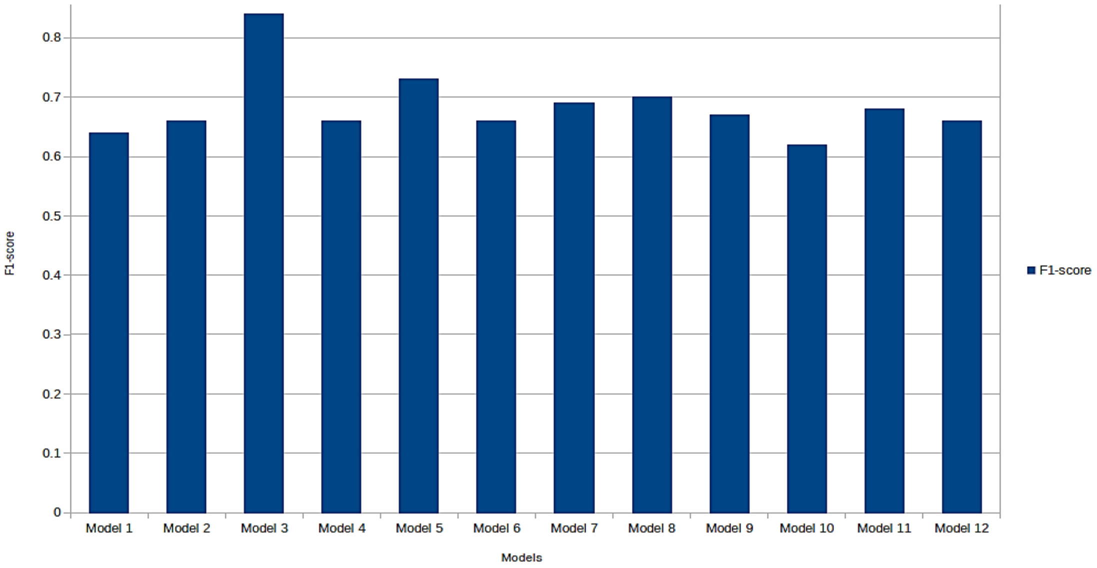

Figure 7. F1-score results of DNN models

5. CONCLUSION

In this paper, we have applied DNN algorithm in KBID to detect two of important members of the several DDoS attack categories: data/UDP flooding and SYN flooding attacks in MANETs. Our model was trained and evaluated with CICDDoS2019 dataset, it is purely dedicated to DDoS attacks, with a large number of transaction network records. According to the environment of MANETs, the obtained results with DNN of maximum three deep hidden layers with 39 hidden nodes, learning rate 0.001 and he_uniform function for Weight initialization, are so promoting. As a perspective, we will continue this research by upgrading the proposed IDS to identify other attacks in MANETs using a deep learning method and find a solution to solve the problem of detection of zero-day attacks.

REFERENCES

[1] G. Li, Q. Sun, L. Boukhatem, J. Wu, and J. Yang, “Intelligent vehicle-to-vehicle charging navigation for Mobile electric vehicles via VANET-based communication,” *IEEE Access*, vol. 7, pp. 170888–170906, 2019, doi: 10.1109/ACCESS.2019.2955927.

[2] A. Lamssaggad, N. Benamar, A. S. Hafid, and M. Msahli, “A survey on the current security landscape of intelligent transportation systems,” *IEEE Access*, vol. 9, pp. 9180–9208, 2021, doi: 10.1109/ACCESS.2021.3050038.

[3] B. K. Tripathy, S. K. Jena, V. Reddy, S. Das, and S. K. Panda, “A novel communication framework between MANET and WSN in IoT based smart environment,” *Int. J. Inf. Technol.*, vol. 13, no. 3, pp. 921–931, Jun. 2021, doi: 10.1007/s41870-020-00520-x.

[4] D. S. Lakew, U. Sa’ad, N.-N. Dao, W. Na, and S. Cho, “Routing in flying Ad Hoc networks: A comprehensive survey,” *IEEE Commun. Surv. Tutorials*, vol. 22, no. 2, pp. 1071–1120, 2020, doi: 10.1109/COMST.2020.2982452.

[5] R. Datta and N. Marchang, “Security for mobile ad hoc networks,” in *Handbook on Securing Cyber-Physical Critical Infrastructure*, Elsevier Inc., 2012, pp. 147–190.

[6] J. Marietta and B. C. Mohan, “A review on routing in internet of things,” *Wirel. Pers. Commun.*, vol. 111, no. 1, pp. 209–233, Mar. 2020, doi: 10.1007/s11277-019-06853-6.

[7] X. Shen, R. Fantacci, and S. Chen, “Internet of vehicles [scanning the Issue],” *Proc. IEEE*, vol. 108, no. 2, pp. 242–245, Feb. 2020, doi: 10.1109/JPROC.2020.2964107.

[8] K. Scarfone and P. Mell, “Guide to intrusion detection and prevention systems (IDPS) (Draft),” 2012.

[9] S. Kumar and K. Dutta, “Intrusion detection in mobile ad hoc networks: techniques, systems, and future challenges,” *Secur. Commun. Networks*, vol. 9, no. 14, pp. 2484–2556, Sep. 2016, doi: 10.1002/sec.1484.

[10] K. Khan, A. Mehmood, S. Khan, M. A. Khan, Z. Iqbal, and W. K. Mashwani, “A survey on intrusion detection and prevention in wireless ad-hoc networks,” *J. Syst. Archit.*, vol. 105, May 2020, doi: 10.1016/j.sysarc.2019.101701.

[11] O. Sbai and M. Elboukhari, “Classification of mobile Ad Hoc networks attacks,” in *2018 IEEE 5th International Congress on Information Science and Technology (CiSt)*, Oct. 2018, vol. 2018, pp. 618–624, doi: 10.1109/CIST.2018.8596391.

[12] O. Sbai and M. Elboukhari, “Data flooding intrusion detection System for MANETs using deep learning approach,” in *Proceedings of the 13th International Conference on Intelligent Systems: Theories and Applications*, Sep. 2020, pp. 1–5, doi: 10.1145/3419604.3419777.

[13] O. Sbai and M. Elboukhari, “Intrusion detection system for manets using deep learning approach,” *Int. J. Comput. Sci. Appl.*, vol. 18, no. 1, pp. 85–101, 2021.

[14] P. Rani, Kavita, S. Verma, and G. N. Nguyen, “Mitigation of black hole and gray hole attack using swarm inspired algorithm with artificial neural network,” *IEEE Access*, vol. 8, pp. 121755–121764, 2020, doi: 10.1109/ACCESS.2020.3004692.

[15] F. Feng, X. Liu, B. Yong, R. Zhou, and Q. Zhou, “Anomaly detection in ad-hoc networks based on deep learning model: A plug and play device,” *Ad Hoc Networks*, vol. 84, pp. 82–89, Mar. 2019, doi: 10.1016/j.adhoc.2018.09.014.

[16] Y. Zeng, M. Qiu, D. Zhu, Z. Xue, J. Xiong, and M. Liu, "DeepVCM: A deep learning based intrusion detection method in VANET," in *2019 IEEE 5th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing, (HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS)*, May 2019, pp. 288–293, doi: 10.1109/BigDataSecurity-HPSC-IDS.2019.00060.

[17] A. Shiravi, H. Shiravi, M. Tavallaee, and A. A. Ghorbani, "Toward developing a systematic approach to generate benchmark datasets for intrusion detection," *Comput. Secur.*, vol. 31, no. 3, pp. 357–374, May 2012, doi: 10.1016/j.cose.2011.12.012.

[18] G. F. Riley and T. R. Henderson, "The ns-3 network simulator," in *Modeling and Tools for Network Simulation*, Berlin: Springer Berlin Heidelberg, 2010, pp. 15–34.

[19] R. A. Sowah, K. B. Ofori-Amanfo, G. A. Mills, and K. M. Koumadi, "Detection and prevention of man-in-the-middle spoofing attacks in MANETs using predictive techniques in artificial neural networks (ANN)," *J. Comput. Networks Commun.*, vol. 2019, pp. 1–14, Jan. 2019, doi: 10.1155/2019/4683982.

[20] K. M. A. Alheeti and K. McDonald-Maier, "Intelligent intrusion detection in external communication systems for autonomous vehicles," *Syst. Sci. Control Eng.*, vol. 6, no. 1, pp. 48–56, Jan. 2018, doi: 10.1080/21642583.2018.1440260.

[21] S. Vimala, V. Khanaa, and C. Nalini, "A study on supervised machine learning algorithm to improvise intrusion detection systems for mobile ad hoc networks," *Cluster Comput.*, vol. 22, no. S2, pp. 4065–4074, Mar. 2019, doi: 10.1007/s10586-018-2686-x.

[22] O. Sbai and M. Elboukhari, "A simulation analyses of MANET's attacks against OLSR protocol with ns-3," in *Innovations in Smart Cities Applications Edition 3*, M. Ben Ahmed, A. A. Boudhir, D. Santos, M. El Aroussi, and \.Ismail Rak\ip Karas, Eds. Cham: Springer International Publishing, 2020, pp. 605–618.

[23] S. Kristiansen, "Ns-3 tutorial," pp. 1–48, 2010, [Online]. Available: https://www.uio.no/studier/emner/matnat/ifi/INF5090/v11/undervisningsmateriale/INF5090-NS-3-Tutorial-2011-Oslo-slides.pdf.

[24] C. Perkins, E. Belding-Royer, and S. Das, "RFC3561: Ad hoc on-demand distance vector (AODV) routing," RFC Editor, Jul. 2003. doi: 10.17487/rfc3561.

[25] T. Clausen and P. Jacquet, "RFC3626: Optimized link state routing protocol (OLSR)," RFC Editor, Oct. 2003. doi: 10.17487/rfc3626.

[26] A. Nadeem and M. P. Howarth, "A survey of MANET intrusion detection & prevention approaches for network layer attacks," *IEEE Commun. Surv. Tutorials*, vol. 15, no. 4, pp. 2027–2045, 2013, doi: 10.1109/SURV.2013.030713.00201.

[27] I. Sharafaldin, A. H. Lashkari, S. Hakak, and A. A. Ghorbani, "Developing realistic distributed denial of service (DDoS) attack dataset and taxonomy," in *2019 International Carnahan Conference on Security Technology (ICCST)*, Oct. 2019, pp. 1–8, doi: 10.1109/CCST.2019.8888419.

[28] A. H. Lashkari, G. D. Gil, M. S. I. Mamun, and A. A. Ghorbani, "Characterization of tor traffic using time based features," in *Proceedings of the 3rd International Conference on Information Systems Security and Privacy*, 2017, vol. 2017, pp. 253–262, doi: 10.5220/0006105602530262.

[29] Y. Cai, H. Zhang, and Y. Fang, "A conditional privacy protection scheme based on ring signcryption for vehicular Ad Hoc networks," *IEEE Internet Things J.*, vol. 8, no. 1, pp. 647–656, Jan. 2021, doi: 10.1109/JIOT.2020.3037252.

BIOGRAPHIES OF AUTHORS

Oussama Sbai is a PhD candidate in computer science at Mohammed 1st University, Oujda, Morocco. His research interests include network security and network IDS using machine learning and deep learning. He can be contacted at email: o.sbai@ump.ac.ma.

Mohamed Elboukhari received the DESA (diploma of high study) degree in numerical analysis, computer science and treatment of signal in 2005 from the faculty of Science, Mohammed 1st University, Oujda, Morocco. He is currently professor, department of Applied Engineering, ESTO, Mohammed 1st University, Oujda, Morocco. His research interests include cryptography, quantum cryptography and wireless network security, Mobile Ad Hoc Networks (MANETs). He can be contacted at email: elboukharimohamed@gmail.com.