Online-Journals.org

iJIM International Journal of Interactive Mobile Technologies

iJIM | eISSN: 1865-7923 | Vol. 17 No. 19 (2023) | OPEN ACCESS

https://doi.org/10.3991/ijim.v17i19.27663

PAPER

An Effective Intrusion Detection in Mobile Ad-hoc Network Using Deep Belief Networks and Long Short-Term Memory

Abdulfatai Shola Hanafi[1], Yakub Kayode Saheed[2,3](✉), Micheal Olaolu Arowolo[4,5]

[1]Department of Computer Science, Al-Hikmah University, Ilorin, Nigeria

[2]Department of Computer Science, School of IT & Computing, American University of Nigeria, Yola, Nigeria

[3]Kaptain A. I & Innovation Research Group

[4]Landmark University, Omu-Aran, Nigeria

[5]Landmark University SDG 9 (Industry, Innovation, and Infrastructure Research Group), Omu-Aran, Nigeria

yakubu.saheed@aun.edu.ng

ABSTRACT

A Mobile Ad-hoc Network (MANET) is a self-organizing collection of mobile devices communicating in a distributed fashion across numerous hops. MANETs are an appealing technology for many applications, including rescue operations, environmental monitoring, tactical operations, and so on, because they let people communicate without the usage of permanent infrastructure. This flexibility, however, creates additional security vulnerabilities. Because of its benefits and expanding demand, MANETs have attracted a lot of interest from the scientific community. They do, however, seem to be more vulnerable to numerous attacks that wreak havoc on their performance than any network. Traditional cryptography techniques cannot entirely defend MANETs in terms of fresh attacks and vulnerabilities due to the distributed architecture of MANETs; however, these issues can be overcome by using machine learning approaches-based intrusion detection systems (IDS). IDS, typically screening system processes and identifying intrusions, are commonly employed to supplement existing security methods because preventative techniques are never enough. Because MANETs are continually evolving, their highly limited nodes, and the lack of central observation stations, intrusion detection is a complex and tough process. Conventional IDSs are difficult to apply to them. Existing methodologies must be updated for MANETs or new approaches must be created. This paper aims to present a novel concept founded on deep belief networks (DBN) and long short-term memory (LSTM) for MANET attack detection. The experimental analysis was performed on the probe, root to local, user to root, and denial of service (DoS) attacks. In the first phase of this paper, particle swarm optimization was used for feature selection, and subsequently, the DBN and LSTM were used for the classification of attacks in the MANET. The experimental results gave an accuracy reaching 99.46%, a sensitivity of 99.52%, and a recall of 99.52% for DBN and LSTM accuracy reaching 99.75%, a sensitivity of 99.79%, and a recall of 99.79%.

KEYWORDS

mobile ad-hoc network, intrusion detection, deep belief network, long short-term memory, particle swarm optimization

Hanafi, A.S., Saheed, Y.K., Arowolo, M.O. (2023). An Effective Intrusion Detection in Mobile Ad-hoc Network Using Deep Belief Networks and Long Short-Term Memory. *International Journal of Interactive Mobile Technologies (iJIM)*, 17(19), pp. 123–135. https://doi.org/10.3991/ijim.v17i19.27663

Article submitted 2021-11-09. Revision uploaded 2022-11-14. Final acceptance 2023-08-11.

1 INTRODUCTION

Along with the rapid adoption of lower-cost, smaller, and more capable wireless nodes in recent years, mobile ad-hoc networks (MANETs) have garnered considerable interest, establishing them as among the most promising fields of wireless network growth [1], [2]. Ad hoc networks are widely utilized in wireless systems and are employed in a wide variety of contexts, spanning rescue operations, personal area networking, disaster relief, and a variety of business, scientific, and defense applications [3]. Due to the current proliferation of cutting-edge technology, MANETs have garnered a considerable reputation in recent years [4]. MANETs, which feature self-maintenance, self-configuration, low-cost deployment, are collections of mobile nodes that rely on one another to transport packets and extend the mobile nodes' restricted transmission ranges. The MANET doesn't require any additional infrastructure to be deployed and is extremely inexpensive to implement anywhere [5], [6].

Typically, MANETs do not rely on centralized equipment like routing backbones or fixed routers. There are no connected wires. As a result, nodes are limited to communicating with nodes in their communication range. Because MANET nodes can freely join and leave networks, network elements are unpredictable. It's worth noting that, because wireless technology utilizes open transmission means, monitoring is quite straightforward. Additionally, the absence of a coordinated and unified dubious filtering infrastructure poses significant security challenges for MANETs. As a result, MANETs are especially susceptible to assault. When a source node wishes to transfer packets of data to a destination node over a medium that is open, it employs multi-hop transmission with the assistance of a relay node. Considering the unstructured network, dynamic topology, open media, and great movement of the nodes, hostile nodes can readily infiltrate the network [7].

Malicious nodes attempt to disrupt network resources by dropping data packets, stealing critical information, or modifying data packets, all of which result in unwanted situations[8], a phenomenon referred to as a Denial of Service (DoS) attack[9]. A DoS is an occurrence that impairs or removes a network's ability to execute its intended purpose. The objective is to deprive nodes' interaction of network capacity, resulting in data packets being dropped and bandwidth being reduced, by prohibiting people from accessing resources [10].

A DoS assault is among the greatest famous kinds of network intrusion, to degrade the service offered by a particular target to other genuine customers [11], [12], [13]. There are various types of DoS attacks, including blackhole, wormholes, flooding, and gray hole [14], [15], [16], [17]. Each leverages a unique security flaw in the network and wreaking havoc on variables like connection interruption, traffic flooding, system interruption, and access blocking in the wireless link [18]. The initial three assaults outlined above alter the system's behavior of routing by fabricating and modifying routing pathways. In contrast to the other approaches, flooding attacks target specific network users by sending a large number of bogus data. According to [19], a flooding assault can reduce the packet distribution ratio by much to 84 percent. The UDP flooding assault [20] is a type of data syn flood assault in which the chosen target is overrun by a constant stream of data circulation at a higher bit rate and packet scope than normal. IDS are used to monitor and identify network infractions to recognize and respond to them [21]. As a result, it is critical to successfully implement and manage such systems to assure the integrity and availability of network services [19] [22].

The remainder of the paper is laid out as follows. The related work was described in Section 2. The recommended approach is then presented in Section 3, followed

by the evaluation data gathered through experiments and comparative studies in Section 3. Finally, in Section 4, the conclusion is offered.

2 RELATED WORK

To reveal separate sorts of DoS attacks, ref. [23] presented a cross-layer IDS. They've also used data mining and clustering methods to Figure out how often intrusive activity occurs. When compared to other existing models, this technique results in faster detection of unlawful activities.

Ref. [24] gives another intriguing paper that continues the trend of association-rule (ARM) mining for IDS in the MANET ecosystem. They've released a cross-layer ID framework that can identify malicious networks and other sorts of DoS assaults. This method uses a fixed-width clustering method to capture harmful behavior in MANETs properly. In Moradi et al., [25] the authors presented ANNs used in the MANET viewpoint. They described a neural network-based IDS in MANET for detecting DoS assaults. To capture DoS attacks, the experimental stage is carried out in a virtual MANET setting while reviewing the outcomes of ANN modeling. This set of works gives evidence that the method used can efficiently achieve a high degree of detection for DoS assault. Abdel-Fattah et al. [26] describe an application of IBL in the domain of IDS for MANET. Traditional systems have struggled to gather real-time attacks, prompting scientists to find and resolve the issue by inventing a new intrusion mechanism to reliably identify fraudulent efforts in MANET. The research shows that the unique method can detect anomalous behaviors with small positive percentages whilst attaining a greater detection rate, based on experimental results. In MANET, the authors [27] investigated the K-NN technique further. The goal of this research is to develop a novel intrusion detection model for MANET. To categorize the audit's foreknowledge for anomaly detection, this model uses the CP-KNN algorithmic approach. With the highest accuracy rates, high confidence rate, and a low false-alarm rate, the unique work indicates the accurate detection of many anomalies. Lately, a method for noticing DoS assaults in WMN was developed [28]. The algorithm's performance was tested using average packet drop rate, delay metrics, and packet delivery ratio. By including a priority system in the system, it has remained demonstrated that the projected IDS positively remove malevolent nodes and boost the packet distribution ratio while decreasing the drop of the packet. To track down fraudulent nodes in MANET, a novel tracing approach dubbed ZSBT has been suggested [29]. Before forwarding a packet, nodes insert the area ID into it with a particular frequency using the suggested algorithm. In these instances, the rogue node's identification is inaccurate. SVMs were studied in detail in [30] to detect DoS assaults. The suggested method's performance has been experimentally confirmed, demonstrating that the proposed SVM-based detection methodology provides extremely high accuracy. Ref. [31] proposes a proactive detection approach for DDoS threats with reduced processing complexity. Additionally, a thorough examination of routing assaults and their countermeasures in MANET can be discovered in [17], [14]. The articles conduct reviews of IDS and discuss their fortes and weaknesses. Other systems for dealing with DoS and DDoS assaults in MANETs have been proposed [32], [18]. The earlier suggestions are primarily based on methods that consider a single network attribute, such as hello-interval attack delay [18], or the answer is limited to a single routing algorithm [32]. Hence, the major gaps noticed in previous studies, such as improving the limiting feature selection for data collecting, must be filled. Another issue noticed in existing works is the focus on one specific assault.

Contrary to previous attempts, this paper proposed an FS approach based on PSO for feature selection as against existing studies. The DBN and LSTM models were utilized for the classification of the probe, user-to-root, root-to-local, and DoS attacks as against previous studies that focused on only the DoS attack.

2.1 Proposed DL-IDS for MANET

The proposed DL-IDS is made up of four modules; the collection of data module, a feature selection module, a detection engine module, and a response module. The data collection module feeds the PSO for feature selection operation. The FS feeds the detection engine module with the necessary network facts for specialized data analysis, and the response module acts on the detection engine module's output [33]. Each of the modules is created in stages, with the demands of the ultimate system in mind.

2.2 Collection of data module

The criterion collected in this section is determined by the type of threat to be alleviated. Each type of network interruption impacts distinct system performance factors, and different types of the user to root, probe, remote to local, DoS assaults necessitate different detection and neutralization strategies. When a misbehaving node floods the target in a MANET, it causes a substantial rise in the packets number targeted at the destination per unit of time, effectively outsourcing the target and exceeding the bandwidth boundary which leads to packet drops frequently.

2.3 Feature selection module

The method began with the acquisition of a dataset, followed by data filtering and normalization, which helps to eliminate inconsistent and outlier data. Finally, PSO was used to select the best fraction solution from the dataset, after which the data was separated into two parts: training and testing.

2.4 Detection engine module

The detection module is at the heart of the IDS system and has a significant impact on its performance. It can be created with the help of special algorithms, an ML model, or any ANN [34]. The architecture of the proposed system is given in Figure 1. Nodes (N) contribute to conventional MANET parts such as receiving and delivering data during normal operation, as shown in Figure 2. The destination base (D) collects and processes packets of data without difficulty. Figure 3 depicts a hypothetical circumstance in which the system is under attack. In this case, network nodes (N) keep functioning normally; however, the offending node (A) begins sending a large volume of useless data to its victim (D), which gradually ceases to function properly, resulting in many node failures and delayed signal arrival. The intrusive and normal data statistics are used to train the DBN and LSTM detection modules. The mean of one-second periods is used to calculate the statistics of each feature. The data is separated into test and training portions, which are then normalized and used as the system's input. Because the detection unit has been taught to learn how the network behaves under normal and attack settings, large departures from the norm are labeled as an intrusion.

The system has been tested with various nodes in the network and its performance is verified after teaching the detection module with five nodes.

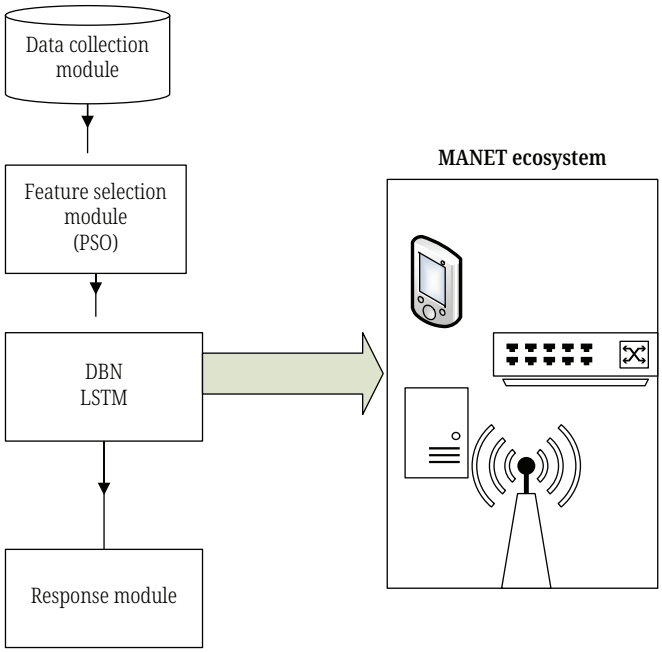

Fig. 1. The architecture of the PSO + DBN-LSTM for IDS-MANET

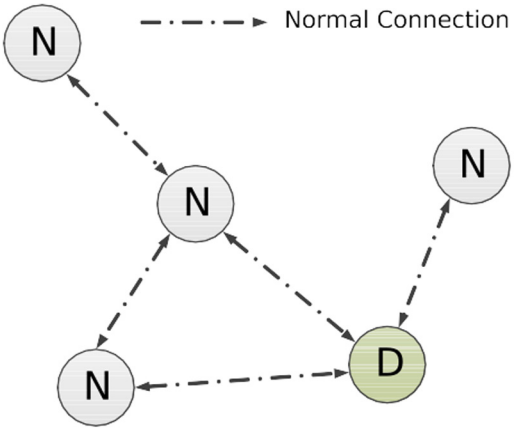

Fig. 2. An example of a MANET environment [35]

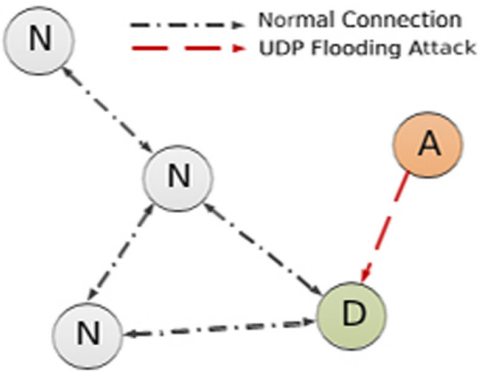

Fig. 3. A MANET amid a DoS assault using UDP flooding [35]

2.5 Response module

The detection module sends the DBN-IDS and LSTM-IDS output to the response module, which makes the ultimate decision. After processing the inputs, the final response is formed, and the relevant actions are taken. Before reacting to the detection module's output, two crucial considerations must be taken into account: the detection module's precision and the potential patterns of future DoS assaults.

2.6 Particle swarm optimization

Particle Swarm Optimization (PSO) is a swarm intelligence-based numerical optimization technique developed by social psychologist James Kennedy and electrical engineer Russell Eberhart in 1995 [36]. PSO is a metaheuristic optimization algorithm paradigm that has garnered popularity in recent years because of its ease of use in unstructured, large high-dimensional data that cannot be handled with classic algorithms [37]. PSO stands for "particle swarm optimization". A set of completely random potential solutions is used to carry out this search. A swarm is a cluster of potential solutions, and each viable solution is referred to as a particle. The search in PSO is impacted by two forms of particle learning. During the motion, each particle learns from other particles as well as from its own experience. Learning from others is referred to as social learning, whereas learning from one's own experience is referred to as cognitive learning. As a consequence of social training, the particle remembers the best solution that any particle in the swarm has visited, which we refer to as gbest [36]. As a consequence of learning skills, the particles save the best answer it has found so far in their memory, dubbed pbest. Figure 4 shows a typical geometric representation of a particle's motion in two dimensions.

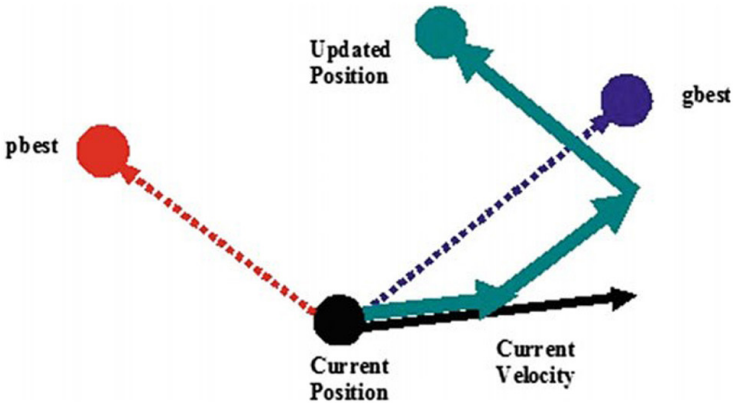

Fig. 4. Particle movement in the PSO process as a geometric illustration [36]

2.7 Deep belief network

The DBN [38], a probabilistic generative system, is a deep neural network classifier that combines RBM [39], a multilayer unsupervised learning network, and BP [39], a supervised learning network. Figure 5 depicts a multilayer generative model with symmetric unguided links in the two highest layers and directed top-down interconnections from the level above in the lower layers [40]. The recognition system is represented by the upward arrows, while the generative model is represented by the downward

arrows [41]. A graphical model of a DBN having m levels can be created. The following is the joint probability of the position as a leading u and the hidden layer i_j for $j = 1{:}m$.

$$p(u, i_1, \ldots, i_m) = p(u \mid i_1) \prod_{m=2}^{j=1} P(i_j \mid i_{j+1})\, p(i_{m-1} \mid i_m) \tag{1}$$

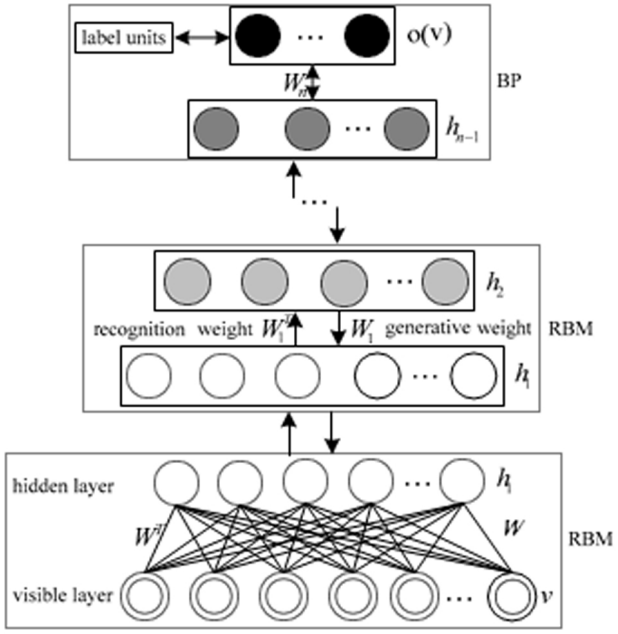

Fig. 5. A DBN and its parameters [41]

2.8 Long short-term memory

The LSTM is a type of recurrent neural network [42]. Hochreiter and Schmidhuber introduced LSTM in 1997 [43]. LSTM are recurrent neural networks (RNNs), which are neural networks with at least one cycle in their underlying structure of inter-neuronal connections. LSTM is designed primarily to understand long-term connections and can overcome the challenges that RNNs had previously [44]. An input layer, one or even more concealed units, and a production (output) layer comprise an LSTM network. The LSTM is arranged in a chain structure. The recurring module, on the other hand, has a unique structure. It features four cooperating levels with a unique form of communication, rather than a single neural network like a normal RNN [45]. Figure 6 showed the diagrammatic representation of LSTM memory cell structure.

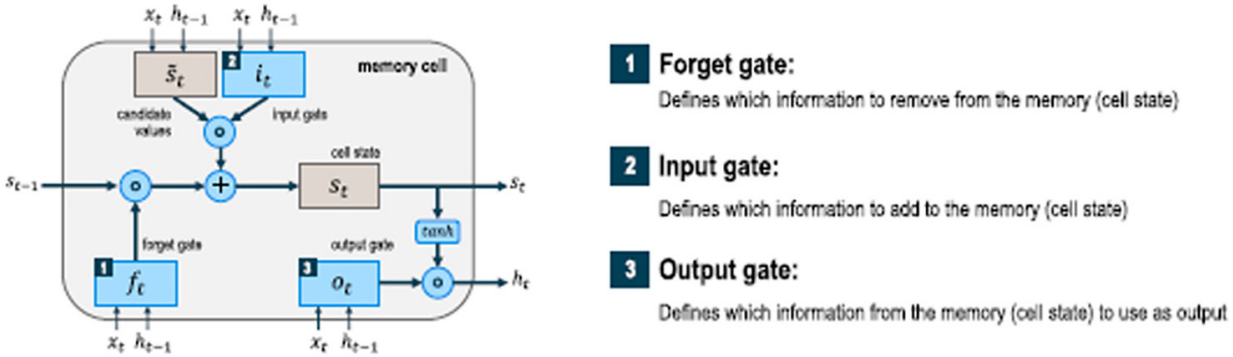

Fig. 6. The LSTM memory cell's structure [44]

3 RESULTS AND DISCUSSION

The system was created to select an efficient DL model for ID in MANET, and this section offers the analysis of the results of the DBN and LSTM methodologies utilized for the experimentation of this research. Among the DBN and LSTM, the experimental model aims to find the best DL classification approach. The training and testing set of data was split in half and passed to DBN and LSTM classifiers, respectively, at a percentage ratio of 75 percent and 25%. Machine learning statistical variables such as classification accuracy, true positive rate, false-negative rate, error rate, specificity, sensitivity, and training duration were used to analyze the outcomes.

3.1 Experimental performance of DBN classification phase

Table 1 lists the DBN classification evaluation parameters for reduced features based on the accuracy, sensitivity, f-score, specificity, recall, and error rate.

Table 1. Performance of the DBN model

Technique	Accuracy	Sensitivity	F-Score	Specificity	Recall	Error Rate
DBN	99.46	99.52	98.79	97.75	99.52	0.5399

3.2 DBN results of system computational time

The actual computing time spent training and processing the DBN for training the dataset is recorded in Table 2, and it is expressed in total seconds spent on the training process.

Table 2. Training of DBN model

Timing Results	Training Time
DBN	58.53

3.3 Experimental performance of the LSTM classification phase

Table 3 displays the LSTM classification's evaluation criteria for reduced features based on the accuracy, sensitivity, f-score, specificity, recall, and error rate.

Table 3. Performance of the LSTM model

Technique	Accuracy	Sensitivity	F-Score	Specificity	Recall	Error Rate
LSTM	99.75	99.79	99.46	99.01	99.79	0.2413

3.4 LSTM results of system computational time

The actual computing time spent training and processing the LSTM network for training the dataset is calculated in seconds. Table 4 summarizes the findings.

Table 4. LSTM training time

Timing Results	Training Time
LSTM	52.33

3.5 Comparative evaluation of DBN and LSTM models

Table 5 illustrates the f-score, specificity, sensitivity, accuracy, and error rate evaluation metrics for the DBN and LSTM models.

Table 5. Evaluation of the performance of the DBN and LSTM models

Techniques	Accuracy	Sensitivity	F-Score	Specificity	Recall	Error Rate
DBN	99.46	99.52	98.79	97.75	99.52	0.5399
LSTM	99.75	99.79	99.46	99.01	99.79	0.2413

The classification accuracy demonstrates that the LSTM network model achieved the best classification rate, implying that the LSTM performed most effectively. Figure 7 showed that the LSTM outperformed the DBN in terms of accuracy, sensitivity, F-score, specificity, and recall while the LSTM model indicates lower error as compared to the DBN network.

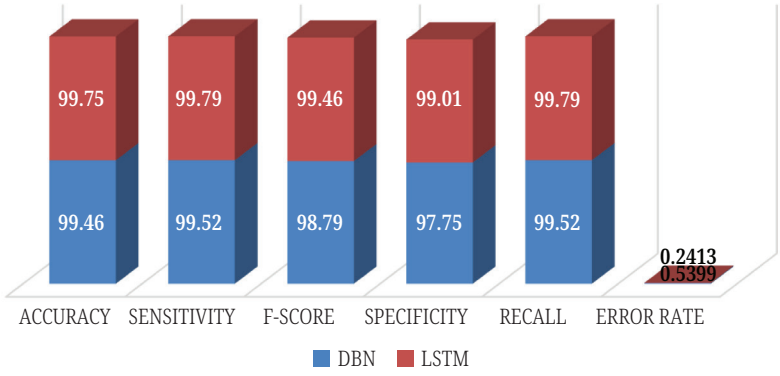

Fig. 7. Comparative evaluation of DBN and LSTM

3.6 Performance of sensitivity vs specificity

The number of right positive predictions divided by the total number of positives is used to compute Sensitivity (SN), whereas the number of correct negative predictions divided by the total number of negatives is used to determine Specificity (SP). The best sensitivity and specificity fall at 1. The obtained results show the sensitivity and the specificity rate have a value close to 1, indicating a good predictive rate. The LSTM proved better than its counterpart as its specificity and sensitivity equate to 1. Figure 8 depicts the metrics of sensitivity and specificity.

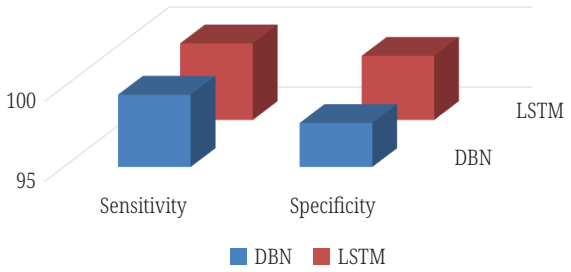

Fig. 8. Sensitivity and specificity metrics

4 CONCLUSION AND FUTURE WORK

MANETs are a far more appealing target for a multitude of different decentralized threats, which generally target the protocol stack's network and data link layers. As a result, deploying an IDS as a second line of protection in MANETs is critical. While authentication and encryption measures may safeguard in some ways, such as lowering the number of invasions, they cannot guard against unknown or unique threats. In this scenario, a deep-learning solution aids in the detection of previously undetected intrusive activity. In this research, we offer MANET detection methods based on DBN and LSTM. The PSO was used for feature selection, while the DBN and LSTM networks were used for the classification of MANET attacks. The results findings showed that the LSTM model gave an outstanding performance when compared with the DBN model. This study identified PSO-LSTM and PSO-DBN as promising AI techniques for estimating attacks in a MANET environment. Especially in the proposed PSO-LSTM model, they could predict the attacks with high reliability.

However, the field of MANET classification techniques is fairly small. When contrasted with the body of information that researchers have studied in other domains, it isn't as extensive. As a result, we recommend that this area be researched further to improve the classification-based IDS in MANET in future work. Additionally, future work may look into the aspect of addressing the classification of IDS in MANET as a multi-class problem and not as a binary problem as shown in this current study.

5 REFERENCES

[1] K. Sumathi and A. Priyadharshini, "Energy optimization in manets using on-demand routing protocol," in *Procedia Comput. Sci*, vol. 47, no. C, 2015, pp. 460–470. https://doi.org/10.1016/j.procs.2015.03.230

[2] W. K. Kuo and S. H. Chu, "Energy efficiency optimization for mobile ad hoc networks," *IEEE Access*, vol. 4, pp. 928–940, 2016. https://doi.org/10.1109/ACCESS.2016.2538269

[3] W. Shim, G. Kim, and S. Kim, "A distributed sinkhole detection method using cluster analysis," *Expert Syst. Appl*, vol. 37, no. 12, pp. 8486–8491, 2010. https://doi.org/10.1016/j.eswa.2010.05.028

[4] Z. A. Zardari *et al.*, "A dual attack detection technique to identify black and gray hole attacks using an intrusion detection system and a connected dominating set in MANETs," *Futur. Internet*, vol. 11, no. 3, 2019. https://doi.org/10.3390/fi11030061

[5] M. S. Pathan, N. Zhu, J. He, Z. A. Zardari, M. Q. Memon, and M. I. Hussain, "An efficient trust-based scheme for secure and quality of service routing in MANETs," *Futur. Internet*, vol. 10, no. 2, 2018. https://doi.org/10.3390/fi10020016

[6] P. S. Hiremath, T. Anuradha, and P. Pattan, "Adaptive fuzzy inference system for detection and prevention of cooperative black hole attack in MANETs," in *Proc. – 2016 Int. Conf. Inf. Sci. ICIS 2016*, 2017, pp. 245–251. https://doi.org/10.1109/INFOSCI.2016.7845335

[7] S. Perumal, "An effectual secured approach against sybil attacks in wireless networks," *Int. J. Interact. Mob. Technol*, vol. 16, no. 9, pp. 217–230, 2022. https://doi.org/10.3991/ijim.v16i09.30213

[8] A. Alsarhan, A. R. Al-Ghuwairi, E. Alshdaifat, H. Idhaim, and O. alkhawaldeh, "A novel scheme for malicious nodes detection in cloud markets based on fuzzy logic technique," *Int. J. Interact. Mob. Technol*, vol. 16, no. 3, pp. 136–150, 2022. https://doi.org/10.3991/ijim.v16i03.27933

[9] P. Roshani and A. Patel, "Techniquesto mitigate grayhole attack in MANET: A survey," in *Proc. 2017 Int. Conf. Innov. Information, Embed. Commun. Syst. ICIIECS 2017*, vol. 2018-January, 2018, pp. 1–4. https://doi.org/10.1109/ICIIECS.2017.8276064

[10] A. Alsumayt, J. Haggerty, and A. Lotfi, "Detect DoS attack using MrDR method in merging two MANETs," in *Proc. – IEEE 30th Int. Conf. Adv. Inf. Netw. Appl. Work. WAINA 2016*, 2016, pp. 889–895. https://doi.org/10.1109/WAINA.2016.113

[11] S. T. Zargar, J. Joshi, and D. Tipper, "A survey of defense mechanisms against distributed denial of service (DDOS) flooding attacks," *IEEE Commun. Surv. Tutorials*, vol. 15, no. 4, pp. 2046–2069, 2013. https://doi.org/10.1109/SURV.2013.031413.00127

[12] N. Schweitzer, A. Stulman, A. Shabtai, and R. D. Margalit, "Mitigating denial of service attacks in OLSR protocol using fictitious nodes," *IEEE Trans. Mob. Comput*, vol. 15, no. 1, pp. 163–172, 2016. https://doi.org/10.1109/TMC.2015.2409877

[13] M. Poongodi and S. Bose, "A novel intrusion detection system based on trust evaluation to defend against DDoS attack in MANET," *Arab. J. Sci. Eng*, vol. 40, no. 12, pp. 3583–3594, 2015. https://doi.org/10.1007/s13369-015-1822-7

[14] 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. https://doi.org/10.1109/SURV.2013.030713.00201

[15] B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato, and A. Jamalipour, "A survey of routing attacks in mobile ad hoc networks," *IEEE Wirel. Commun*, vol. 14, no. 5, pp. 85–91, 2007. https://doi.org/10.1109/MWC.2007.4396947

[16] J. Amudhavel *et al.*, "A survey on intrusion detection system: State of the art review," *Indian J. Sci. Technol*, vol. 9, no. 11, pp. 1–9, 2016. https://doi.org/10.17485/ijst/2016/v9i11/89264

[17] R. H. Jhaveri, S. J. Patel, and D. C. Jinwala, "DoS attacks in mobile ad hoc networks: A survey," in *Proc. – 2012 2nd Int. Conf. Adv. Comput. Commun. Technol. ACCT 2012*, 2012, pp. 535–541. https://doi.org/10.1109/ACCT.2012.48

[18] M. Chhabra and B. B. Gupta, "An efficient scheme to prevent DDoS flooding attacks in mobile ad-hoc network (MANET)," *Res. J. Appl. Sci. Eng. Technol*, vol. 7, no. 10, pp. 2033–2039, 2014. https://doi.org/10.19026/rjaset.7.496

[19] S. Desilva and R. V. Boppana, "Mitigating malicious control packet floods in ad hoc networks," *IEEE Wirel. Commun. Netw. Conf. WCNC*, vol. 4, 2005, pp. 2112–2117. https://doi.org/10.1109/WCNC.2005.1424844

[20] J. Mirkovic, S. Fahmy, and P. Reiher, "Measuring impact of DoS attacks," in *Proc. Deter Community Work. Cyber Secur. Exp.*, 2006, pp. 1–4.

[21] X. Pérez-Palomino, K. Rosas-Paredes, and J. Esquicha-Tejada, "Low-cost gas leak detection and surveillance system for single family homes using Wit.ai, Raspberry Pi and Arduino," *Int. J. Interact. Mob. Technol*, vol. 16, no. 9, pp. 206–216, 2022. https://doi.org/10.3991/ijim.v16i09.30177

[22] 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, 2016. https://doi.org/10.1002/sec.1484

[23] R. S. Bhuvaneswaran, *Adaptive Association Rule Mining Based Cross Layer Intrusion Detection System for MANET*, 2011. https://doi.org/10.5121/ijnsa.2011.3519

[24] V. A. Devi and R. S. Bhuvaneswaran, "Agent based cross layer intrusion detection system," pp. 427–440, 2011. https://doi.org/10.1007/978-3-642-22540-6_41

[25] M. Teshnehlab and A. M. Rahmani, "Implimantaion of neural networks for intrusion detection in MANET," pp. 1102–1106, 2011.

[26] F. Abdel-fattah, "Distributed and cooperative hierarchical intrusion detection on MANETs," vol. 12, no. 5, pp. 32–40, 2010. https://doi.org/10.5120/1673-2257

[27] M. Lalli and V. Palanisamy, "A novel intrusion detection model for mobile ad – hoc networks using CP – KNN," vol. 6, no. 5, pp. 193–201, 2014. https://doi.org/10.5121/ijcnc.2014.6515

[28] G. Akilarasu and S. M. Shalinie, "Wormhole-free routing and DoS attack defense in wireless mesh networks," *Wirel. Networks*, vol. 23, no. 6, pp. 1709–1718, 2017. https://doi.org/10.1007/s11276-016-1240-0

[29] X. Jin, Y. Zhang, Y. Pan, and Y. Zhou, "ZSBT: A novel algorithm for tracing DoS attackers in MANETs," *Eurasip J. Wirel. Commun. Netw*, vol. 2006, no. 1, pp. 1–9, 2006. https://doi.org/10.1155/WCN/2006/96157

[30] S. Mukkamala and A. H. Sung, "Detecting denial of service attacks using support vector machines," *IEEE Int. Conf. Fuzzy Syst*, vol. 2, 2003, pp. 1231–1236. https://doi.org/10.1109/FUZZ.2003.1206607

[31] P. Devi and A. Kannammal, "An integrated intelligent paradigm to detect DDoS attack in mobile ad hoc networks," *Int. J. Embed. Syst*, vol. 8, no. 1, pp. 69–77, 2016. https://doi.org/10.1504/IJES.2016.073754

[32] M. Marimuthu and I. Krishnamurthi, "Enhanced OLSR for defense against DOS attack in ad hoc networks," *J. Commun. Networks*, vol. 15, no. 1, pp. 31–37, 2013. https://doi.org/10.1109/JCN.2013.000007

[33] S. Şen and J. A. Clark, *Intrusion Detection in Mobile Ad Hoc Networks*, 2009, pp. 427–454. https://doi.org/10.1007/978-1-84800-328-6_17

[34] L. Nishani and M. Biba, "Machine learning for intrusion detection in MANET: A state-of-the-art survey," *J. Intell. Inf. Syst*, vol. 46, no. 2, pp. 391–407, 2016. https://doi.org/10.1007/s10844-015-0387-y

[35] E. A. Shams and A. Rizaner, "A novel support vector machine based intrusion detection system for mobile ad hoc networks," *Wirel. Networks*, 2017. https://doi.org/10.1007/s11276-016-1439-0

[36] J. C. Bansal, *Particle Swarm Optimization*. Springer International Publishing.

[37] S. Sengupta, S. Basak, R. Alan, and P. Ii, "Particle swarm optimization : A survey of historical and recent developments with hybridization perspectives," pp. 157–191, 2019. https://doi.org/10.3390/make1010010

[38] G. E. Hinton, S. Osindero, and Y.-W. Teh, "A fast learning algorithm for deep belief nets," *Neural Comput*, vol. 18, no. 7, pp. 1527–1554, 2006. https://doi.org/10.1162/neco.2006.18.7.1527

[39] D. E. Rumelhart and G. E. Hintont, "Learning representations by back-propagating errors," no. 2, pp. 3–6, 1986.

[40] Y. Yang, K. Zheng, C. Wu, X. Niu, and Y. Yang, "Building an effective intrusion detection system using the modified density peak clustering algorithm and deep belief networks," 2019. https://doi.org/10.3390/app9020238

[41] N. Gao, L. Gao, Q. Gao, and H. Wang, "An intrusion detection model based on deep belief networks," in *2014 Second International Conference on Advanced Cloud and Big Data*, Huangshan, China, 2014, pp. 247–252. https://doi.org/10.1109/CBD.2014.41

[42] H. Inoue, H. Ochiai, D. Fall, and Y. Kadobayashi, "Long short-term memory-based intrusion detection system for in-vehicle controller area network bus," pp. 10–17, 2020. https://doi.org/10.1109/COMPSAC48688.2020.00011

[43] S. Hochreiter, "Long short-term memory," vol. 1780, pp. 1735–1780, 1997. https://doi.org/10.1162/neco.1997.9.8.1735

[44] T. Fischer and C. Krauss, "Deep learning with long short-term memory networks for financial market predictions," *Eur. J. Oper. Res*, vol. 270, no. 2, pp. 654–669, 2018. https://doi.org/10.1016/j.ejor.2017.11.054

[45] X. Le, H. V. Ho, G. Lee, and S. Jung, "Application of long short-term memory (LSTM) neural network for flood forecasting," 2019. https://doi.org/10.3390/w11071387

6 AUTHORS

Abdulfatai Shola Hanafi received the master's degree from Al-Hikmah University, Ilorin, Nigeria. He is currently working in the area of data science and analytics.

Yakub Kayode Saheed received a Ph.D. degree in Computer Science from Kwara State University. He is currently Assistant Professor in the Department of Computer Science, School of IT & Computing at the American University of Nigeria. He is co-founder of Kaptain Machine Learning Lab, where he leads the Machine Learning Lab. Dr. Yakub is a member of IEEE, the Internet Society, IAENG, and SDWIC. He has published in several international journals and conference proceedings (ORCID: 0000-0002-0804-0707).

Micheal Olaolu Arowolo received the bachelor's degree from Al-Hikmah University, Ilorin, Nigeria, the master's degree from Kwara State University, Malete Nigeria, and the Ph.D. degree from Landmark University, Omu-Aran Nigeria. He is currently a Faculty Member of the Department of Computer Science, Landmark University. He has published widely in local and international reputable journals. His research interests include machine learning, bioinformatics, datamining, cyber security, and computer arithmetic. He is a member of IAENG, APISE, SDIWC, and an Oracle Certified Expert.