ISSN 2303-4521
Periodicals of Engineering and Natural Sciences *Original Research*
Vol. 10, No. 3, May 2022, pp.70-78

Proposed neural intrusion detection system to detect denial of service attacks in MANETs

Raghad Mohammed Hadi[1], Salma Hameedi Abdullah[2], and Wafaa M. Salih Abedi[3]
[1]Al-Mustansiriya University, College of Medicine, Physiology Branch
[2] University of Technology, Computer Engineering Department
[3]City University College of Ajman, Ajman, UAE

ABSTRACT

MANTs are groups of mobiles hosts that arrange themselves into a grid lacking some preexist organization where the active network environment makes it simple in danger by an attacker. A node leaves out, and another node enters in the network, making it easy to penetration. This paper aims to design a new method of intrusion detection in the MANET and avoiding Denial of Service (DoS) basis on the neural networks and Zone Sampling-Based Traceback algorithm (ZSBT). There are several restrictions in outdating intrusion detection, such as time-intense, regular informing, non-adaptive, accuracy, and suppleness. Therefore, a novel intrusion detection system is stimulated by Artificial Neural Network and ZSBT algorithm using a simulated MANET. Using KDD cup 99 as a dataset, the experiments demonstrate that the model could can detect DoS effectively.

Keywords: MANET, DOS attack, echo state network (ESN), Intrusion detection, Zone-Sampling-Based Traceback algorithm (ZSBT).

Corresponding Author:

Raghad Mohammed Hadi
College of Medicine, Physiology Branch
Al-Mustansiriya University
Baghdad, Iraq
raghad_alrudeiny@uomustansiriyah.edu.iq

1. Introduction

The conception of MANET is the collection of wireless mobiles host lacking by every cable, substructure, and construction. All mobile nodes in this system perform direction-finding, which prepares the responsibilities of packets transfer and packets getting in cooperation. MANET preparation does not necessitate central management or mobile network substructures; such as corrupted positions or access facts. A MANET is an independent collection of mobile operators that connect ended sensibly measured wireless relations. The net topology might differ in fast and randomly ended times, as the nodes mobile. Such a net might work in a separated style or be linked to the greater Internet. MANETs have certain features similar to Bandwidth forced, adjustable volume links, Energy forced Process, Inadequate Bodily Safety, Active system topology, and recurrent routing inform [1]. Several varieties of attacks contain danger the MANET. For example, Dark holes, Direction finding loops, System Divider, self-centeredness, Slumber Deprivation, and Denial of Service (DoS) are cataloging attacks founded on the importance [2]. An Intrusion Detection System (IDS) is an arrangement of software that notices attacks on a net or system. IDS are usually confidential as Waste and Irregularity discoveries. In the Waste system, the sign of recognized attacks is kept in record. Every data similar to that sign is confidential as attacks. Irregularity discovery denotes numerical information around usual action. Intrusions resemble nonconformities as of the usual activity of method. The irregularity detection method has a great false positive/negative apprehension rate associated with waste detection methods [3, 4].
This paper aims to build a multi-level ID using the foundation of artificial neural networks (ANNs) to notice DoS attacks. ANNs are the approaches that can offer a robust device for noticing malicious nodules in MANET. Great calculation rate, education skill done pattern performance, forecast of unidentified pattern and suppleness insults where the loud patterns are the main benefits of ANNs.

The relaxation of paper is organized as subsequent. In section 2, we discuss the preceding related work. Section 3 explains the KDD cup 99 dataset. Section 4 illustrates the DoS attack. Section 5 displays the ECHO state network. Section 6 describes the ZSBT algorithm. Section 7 shows the proposed system in detail. Section 8 presents the performance evaluation. Section 9 illustrates the trials and results. Finally, section 10 covers the conclusion.

2. Related work

There are many attempts by researchers need to advance IDS by spending ANNs. Some of these searches are described below: Akilandeswari, 2012 [5] planned a method of packet design and entropy in which all packet is noticeable on each router complicated in communiqué in instruction to path the foundation of the packet. Though, a quantity of methods planned via particular journalist's castoff ANN or substructure to protect beside DDOS attacks, anywhere as a pair of them has recognized the basis of the attack. In difference, nobody of them labels every unidentified or nothing attacks branded as great or little dangerous attacks. Henceforth, the chief impartial is to notice and alleviate unidentified Distributed Denial of Services (DDoS) attacks. Ayalakshmi & Santhakumaran [6] proposed a structure named Learning Vector Quantization (LVQ) neural networks to classify attacks. The method is management kind of quantization, which container to use aimed at an additional event like pattern appreciation, data looseness, and multiclass orderings. Also, the contributions were complete to neural networks as datasets in the procedure of arithmetical scheming. Nikita [7] Proposed BPNN as an informal appliance, managed education artificial neural network. Amount of the periods essential to boat train the network was great as a match to the further ANN methods. Then, the discovery rate was actually great. BPNN container was castoff once single needs to not lone notice the attack nonetheless to categorize the attack into an exact group so that the defensive exploit container is occupied. By joining the dissimilar ANN methods, any container decreases the amount of the periods essential and later can decrease the preparation time. The DoS attack resolved in this effort will summarize the amount of the net drive to enhance and net delay. The effort does not need extra hardware and is software-founded. [8] has proposed artificial neural network and ZSBT process founded IDS which were castoff to discover DoS doses in MANET situation. By a reproduction, it was exposed that the perfect container was used to discover DoS attacks. As of the active landscape of the net, the container is susceptible to occurrences, for instance, DoS. Evaluating was assessed for these limitations for every node in the system to notice attacks and their influences. This technique is recognized as a traceback. Traceback only is not sufficient to classify the deceived nodules. So, IDPF is presented to recognize deceived nodules and prevent the system from additional attacks. Thus, the ZSBT algorithm creates improved consequences through the assistance of Zone ID relatively more than the ANN technique.

2.1. Dataset explanation

The KDD cup 99 dataset is a general dataset cast off for assessing intrusion detection algorithms. Forty-one features per label have all associations to determine the association class (whether normal or attack class). A piece of the dataset was separated into numeric and symbolic types, categorized into the following groups (Elementary landscapes, contented landscapes, Time Grounded Transportation Features, Time Grounded Transportation Features). The attack period is categorized into four main groups [9].

- DoS attacks: An invader effort to brand the method reserve busy to avert the valid operator by the system.
- Investigation attack: The invader tests the system to assemble material and discover brittleness. Then, use this brittleness to spasm at advanced times.
- Remote to Local (R2L) attack: The hacker referred the packages to the target device over the net. Later on, the feats brittleness to grow illegal native admission to that device.
- User to Root (U2R) attack: Hacker at principal acquires admission to a standard user then achievements brittleness in the scheme to acquire basis level access. The goal of this occurrence is to acquire illegal operator freedoms. The KDD cup 99 dataset contains a training and testing dataset (see Table 1). There are 4,940,000 data models in the preparation set, and these models are dispersed among usual performance and 24 spasms. On the additional indicator, there are 311,029 data models containing usual system traffic and 38 courses of spasm, 24 occurrences present in the preparation set, and 14 different attacks. As the preparation set encompasses a great amount of data models, other preparation sets moulded contain 10% of facts models castoff in varied range [10].

Table 1. Number of samples in KDD cup 99 dataset

Dataset	Normal	DoS	Probe	U2R	R2L	Total
Corrected KDD 99"	60593	229853	4166	70	1126	311029
"10% KDD	97277	391458	4107	52	1126	494020

Normalization of the dataset has been completed, and thus, it will be suitable to be castoff via the proposed algorithm. The subsequent steps display the normalization process:

1. Alter the rate of representative features to successive numeral values from [1….M], which are the three forms of rules (TCP, UDP, and ICMP), 68 kinds of facility, and 11 kinds of ensign in the KDD cup 99 dataset. Neural network algorithm and ZSBT algorithm receive numerical values.
2. Data standardization can be produced to escape the bias problem at particular greater landscapes values. This indication to advance the competence and the correctness of taking algorithms. These algorithms afford improved consequence when the data to be examined reduction among [0 and 1]. Min-max normalization method, which is a linear alteration, is castoff to ruler data among [0 and 1]. The succeeding formula is castoff to the invention of the novel value [11].

$$\mathbf{X_n = \frac{x - x_{min}}{x_{max} - x_{min}}} \quad \textbf{.... (1)}$$

2.2. Denial of service attack

It is one of the attacks that a cautious, malicious, and illegal challenge to divest valid system customers from expending their system resources. DoS touch facility workers in numerous facets, greatest particularly crippling obtain ability of facilities providing in them [12]. DoS themselves are not influential sufficient to transport depressed any web facility in current computational capitals situation. A more urbane ascendable and distributed occurrence changed from DoS is the DDoS. Computer Incident Advisory Capability principally stated it. Later that period, almost all DoS attacks were some way of dispersed characteristics [13]. DoS can be presented as the following situation: an interloper node vaccinates a large number of jumble packets into the network. This exploit ingests an important helping of network incomes and reasons a rejection of the criticized node's services could deliver for additional nodes [14].

2.3. Echo state network

An Echo State Network (ESN) arbitrarily makes a great linked RNN (a reservoir) determined through training contribution indication and development to production units. Just the educated links are the reservoir to production units in the education procedure. Informing the reservoir situations and network productions are achieved to give the following equations [15]:

$A(t+1)=(1-\beta) * Ƒ(W_r A(t)+ W_{in} u(t+1) + \beta * A(t)$ ……. (2)

$B(t+1)= Ƒ_{out}(W_{readout}[A(t+1); u(t+1)])$ …… …. (3)

where A(t) is the reservoir general at period t, and β≥ 0 is the detainment amount of the reservoir. W_r refers to the reservoir weight array, and u(t) is the contribution order. B(t) is the forecast production of the readout at period t. W_{in} and $W_{readout}$ readout are the weight arrays of u(t) and B(t), respectively. Ƒ(0)and $Ƒ_{out}$ are correspondingly the motivation purposes of the reservoir and the forecast production. The main disorder for the production layer preparation is the echo state property (ESP), which indicates that early result situations should be washed out after a time step [16].

2.4. Zone sampling-based traceback algorithm (ZSBT)

In this type of algorithm, the network is divided into zones. Additionally, a node advancing a packet length ways with IP address and zone ID as routing protocol is used to create a secure route from source to destination. By retaining IP deceiving, attackers can avoid discovery. However, with the assistance of Zone ID, the invader node can be recognized simply, and the network is secure since such attacks [17-19].

3. Proposed system

The proposed system's profound investigation of IDS is accomplished in two phases. In the first phase, the proposed system is trained with the ZSBT algorithm and thus constructing a routing algorithm. This algorithm is used to create a route from source to destination and smear it on the KDD cup 99 dataset in the MANTS network. The proposal has used 3000 records for the training phase and 1900 normal in the dataset. In the second phase, the proposal training with Echo state neural network algorithm partitions the data to various clusters according to reservoir weight matrix with minimum value. The proposal is illustrated in algorithm 1, which shows the system in detail. Figure 1 shows the block diagram for the proposed system.

The network was simulated in the proposed system and created with four nodes. Each node is associated at least to one another node through mobile agents. The mobile agents attend as a communiqué agent between nodes. In the host node, it is exposed to refer several extra jumble packets from the invader node. The treatment of this embrace the traffic tiredness of the host node, then the host node develops incapability to help another node in the network. The DoS attack can be noticed with the assistance of the following parameters:

- Packet loss (PL): It computes the normal quantity of packets released in all time frames on the relations from terminus to swarm node.
- Packet Sending (PS): It computes the normal quantity of packets directed among two nodes, and displays swarm the movement load of swarm nodes.
- Packet Receiving (PR): It computes the normal quantity of conventional packets in all time frames.
- Energy Consumption (EC): The DoS attack might use the battery-operated influence of the terminus node. It events the quantity of vitality each node devours in all time frames. These limitations have to be examined. So, a model communiqué is to be achieved among two nodes.

The factors (PL, PS, PR, and EC) stayed removed by examining log files. The largest and smallest of each contribution and production factor are shown in Table 2. As we say that the proposed system contains two phases explained as follows:

Phase 1: ZSBT algorithm used to route the packet as secure from source to destination, as illustrated in algorithm 2.

Phase 2: Echo state neural network algorithm used to cluster the type of attack categories into the DoS attack or unknown attack where algorithm 3 explains it.

Table 2. MANET confirmation in the proposed system

Factor	Description
Broadcast Range	230 m
Node Location	Random
Imitation Area	200*200
Nominal Speed	1 m/s
Greatest Speed	5 m/s
Scope Of Files Packets	512 bytes
Imitation Time	200 s
Quantity Of Node	4
Strictures	PL, PS, PR, and EC

Algorithm (1): The proposal of IDS
Input: Training dataset
Output: classify the dataset into two classes and cluster the type of attack into their subclass.
Begin

Steps:

1- Apply discretization pre-processing to convert continuous features in the dataset into discrete ones. The MANTs twitches at period p=1 with any random starting formal A(0)=0, the contribution signal u(p) and the internal situations A(p)=($A_1(p), \ldots\ldots A_I(p)$) for p=1500,…, P are composed into an array MM of size (P-1500) * ($N_u + \sum_{i=1}^{I} R_i$) .

2- Computing the output weight matrix
$W_{out}=MM^T(MM * MM^T + €I)^{-1} * D$ where € is regularization coefficient, and I is identity array.

3- //Apply the first level of the proposed system by the following: //
   a) Every input node in the training dataset computes A(t) W_{out} and then goes to algorithm 2.
   b) Repeat until all entry nodes are empty.
   c) End for

4- // Apply the additional level of proposed system//
   a) The output from algorithm2 is used as input to algorithm3.
   b) Repeat until stopping criteria.

5- Allocate the category of attack for all input with maximum value.
6- Separate attack node since standard node rendering to kind of all input pattern
7- End.

Algorithm (2): Zone Sampling-Based Trackback Algorithm.

Input: Number of nodes, node path, zone path, network size, packed size, link cost.

Output: optimal route from source to destination.

Begin
While (node not victim and not the destination) do
Construct a sequence of attack paths by the following:
   a) A packet was received from the node.
   b) Write (zone ID) for the packet.
   c) Calculate the distance from the initial node to the current node.
   d) Forward the packet with (zone ID, distance) to the nearest node.

Else
While (node is the victim and reconstructed the zone path is not complete)
   a) The new value of zone ID was inserted into the attack path sequence.
   b) The path to the victim node will be reflected as a damaged path, and it will be uninvolved from the routing paths of all nodes.
   c) The path from this node to each other nodes will be drawn.
   d) The packets (broadcast) will be invalidated.
   e) Repeat the broadcasting procedure until the destination is found.

End while.
Return optimized route from source to destination.
End.

Algorithm 3: Echo state neural network creating

Input: Number of random node N, number of data point D, number of the weightiness of the teacher outputs *y*(*n*), training dataset.

Output: Detect the type of attack.

Steps

Step 1: Offer an arbitrary Random Dynamical Reservoir by the following steps.

a. By one neuron ideal, the reservoir scope M is needed to generate arbitrary Random Dynamical Reservoir
b. Assign contribution components to the reservoir via generating arbitrary all relations.
c. Generate production components by:
   - In the case of mission, it needs to a production feedback
   - Connect arbitrarily produced production to reservoir networks.
   - In the other case, the mission it does not need production feedback; any network was not generating from or to the production units.

Step 2: Produce Reservoir Situations.

1- Determination of the dynamical Reservoir by the training dataset T for times N = 1,…,N_{max}. Where present: a) the production to reservoir feedback associates, b) these resources to inscribe together, c) the contribution U(N) into the contribution unit, and 4) the educator production *E*(*N*) into the production unit.
2- The reservoir is determined via the contribution U(N) only in the responsibilities lacking production feedback. This consequences in an arrangement X(N) of n dimensional reservoir situations. Every section *X*(*N*) is a nonlinear transmute of dynamic contribution. Each *X*(*N*) is a separate mix of cooperation, the measured step contribution signal, and the wild production.

Step 3: The Compute output weights have the following steps:

a. Calculate the production weights as the direct regression weights of the educator productions *E*(*N*) on the reservoir states.
b. Use the weights to generate *X(N)*to production networks

End

4. Evaluation measures

The capability to brand the accurate detection dependent on the countryside of the assumed status associated with the consequence of intrusion detection system is contingent on the measured efficiency of IDS. The four outcomes are:

1. The right forecast of normal performance was indicated by True negative TN.
2. True positive TP indicated the right forecast of attack performance.
3. A wrong forecast of standard performance as an attack was indicated by False positive FP.
4. False negative FN indicated the mistaken prediction of attack behavior as normal. The four possible results were obtained to correct the performance of the proposed system and were named confusion table, which is described in Table 3.

Table 3. The confusion table

Predicted category	Current category
True negative - TN	Normal
False positive - FP	Normal
False negative - FN	Attack
True positive - TP	Attack

The presentation of the proposed system is appraised by the subsequent procedures described in Table 4.

Table 4. The measure matrix

Measure Performance	Equation	Description
Accuracy (ACC)	$=\frac{TP+TN}{TP+TN+FP+FN}$	The degree of examples that are correctly sensed as standard or attack.

Detection Rate (DR)	$=\frac{TP}{TP+FN}$	The relation of the number of examples that are correctly classified as an attack to the total number of attack samples.
False alarm rate (FAR)	$=\frac{FP}{TN+FP}$	The degree of unsuitably classified examples as an attack to the total quantity of examples of normal performance.

4.1. Experimental results

The KDD99 dataset projected the scheduled system. The planned system was accomplished by examples sensibly designated from KDD 99 dataset. The dataset covers usual presentation examples beyond the added two categories of attack (DoS and unknown) to stipulate usual examples from occurrence samples and similarly to notice the attack category. The proposed system was trained with 41, 25, and 20 structures of the KDD99 dataset, signifying as the structures with maximum Information Gain. In trial 1, the educated prototypical tried with 1000 records holds both normal performance and the other attack types. In trial 2, we have chosen 500 records holds individually standard and attack type castoff to estimate the planned system. The statistics castoff in this effort is shown in Table 5. At the principal level of the proposed system, two estimation criteria are castoff to measure the proposed system (ACC and DR). To check the efficacy of the proposed component, two trials are shown. In the first trials, the algorithm is verified by a dataset called dataset1 consisting of (900) archives compass usual behavior in totaling to other attack categories. The second trials are led by datasets named dataset2 consisting of (400) records correspondingly, and they also contained other types of attack. Table 6 shows the result from the proposed system.

Table 5. dataset used

dataset	record	Number of records
Train	normal	999
Train	DOS	1250
Test1	normal	227
Test1	DOS	452
Test2	normal	138
Test2	DOS	113

Table 6.The result of the proposed system

Dataset	Number of feature	Class type	ACC	DR	FAR
Dataset1	41	normal	0.99	0.98	0.01
Dataset1	25	portsweep	0.91	0.87	0
Dataset1	20	rootkit	0	0	0
Dataset2	41	normal	0.99	1	0.01
Dataset2	25	portsweep	0.88	0.86	0.01
Dataset2	20	rootkit	0.90	1	0.01

5. Conclusion

In this paper, the planned system recognized an intrusion and organization of intrusion in MANETs network. The proposed exertion in the principal level can determine the steady movement from intrusion movement within high precision and discovery rate and small false positive rate, and the additional level can determine the retro of an outbreak with countless discovery rates. The normal movement that is not categorized as an outbreak where in the principal level of the planned system, the container is foreseeable as an unidentified outbreak in the additional phase of the planned system wherever the Echo state neural network algorithm is educated to categorize the standard connection to unknown. The trials presentation shows that the contribution features' measure has affected the haste of the ZSBT algorithm preparation whenever the fewer features of the training time will be reduced.

Declaration of competing interest

The authors declare that they have no any known financial or non-financial competing interests in any material discussed in this paper.

Funding information

No funding was received from any financial organization to conduct this rese

References

[1] P. Sakalley, "Review and Analysis of Various Mobile Ad Hoc Network Routing Protocols," *Ratnaraja Kumar international Journal of Recent Technology and Engineering (IJRTE)*, Vol. 2, No.5, 92-97, 2013.

[2] Z. Moradi, M. Teshnehlab, and A. M. Rahmani, "Implementation of neural networks for intrusion detection in manet," in International Conference on Emerging Trends in Electrical and Computer Technology, 2011.

[3] D. V. R. Harshit Saxena1, " Intrusion Detection System using K- means, PSO with SVM Classifier: A Survey," *International Journal of Emerging Technology and Advanced Engineering Website*, Vol.4, No.2, pp.653-657, 2014 .

[4] A.-K. S. H. N. A. Hadi R. M., " prediction model for financial distress using proposed data mining approach," *journal of Al- Qadisiyah for computer science and mathematics*, Vol.11, No.2, pp.37-44,, 2019.

[5] V. S. S. Akilandeswari, "Probabilistic Neural Network based attack traffic classification," in *Fourth International Conference on Advanced Computing (ICoAC)*, Chennai, 2012.

[6] T. Ayalakshmi and A. Santhakumaran, "Statistical Normalization and Back Propagation for Classification,," *International Journal of Computer Theory and Engineering*, pp. VOL. 3, NO. 1, pp. 89-93, 2011.

[7] S. M. S. M. Nikita1, "To Detect Denial of Service Attack in MANET by ANN Based Technique," *International Journal of Enhanced Research in Science Technology & Engineering*, Vol. 4, No. 5, pp 326-332, 2015.

[8] D. Divya, " Intrusion Detection in MANET using Neural Networks and ZSBT",*International Journal of Computer Applications*, Vol. 81, No.4, pp. 5-10, 2013.

[9] H. M. Nadiammai G.V., "Effective Approach toward Intrusion Detection System using Data Mining Techniques," *Egyptian Informatics Journal*, Vol.15, No.1, pp.37-50, 2014.

[10] S. K. Sahu , " A Detail Analysis on Intrusion Detection Datasets," *IEEE*, pp.1348-1353, 2014.

[11] A. Aljumah, " Detection of Distributed Denial of Service Attacks Using Artificial Neural Networks," *International Journal of Advanced Computer Science and Applications*, Vol. 8, No. 8, 2017.

[12] E. M. Ait and T. Tchakoucht, "Multilayered Echo-State Machine: A Novel architecture for efficient intrusion detection," *IEEE Access*, vol. 6, pp. 72458–72468, 2018.

[13] M. Bhalia, "Analysis of MANET Characteristics, Applications and its routing challenges" ,*international Journal of Engineering Research and General Science*, pp. Volume 3, No. 4, Part-2, 2017.

[14] R. Hadi, N. A. , and S. Abdullah"Propose effective routing method for mobile sink in wireless sensor network", *Periodicals of Engineering and Natural Sciences*, Vol. 8, No. 3, pp.1506-1516, 2020.

[15] H.J. Hassan, and S.H. Abdullah, "Development smart eyeglasses for visually impaired people based on you only look once", *Telkomnika (Telecommunication Computing Electronics and Control)* , vol.20, no.1, pp. 109–117, 2022.

[16] W. M. Salih. "Unconsciousness detection supervision system using faster RCNN architecture" In Proceedings of the 2nd International Conference on Future Networks and Distributed Systems, pp. 1-6. 2018.

[17] Y. S. Mezaal and S. F. Abdulkareem, "Affine cipher cryptanalysis using genetic algorithms," JP Journal of Algebra, Number Theory Applications, vol. 39, no. 5, pp. 785-802, 2017.

[18] I. A. Aljazaery, H. T. Salim ALRikabi, and A. H. M. Alaidi, "Encryption of Color Image Based on DNA Strand and Exponential Factor," International Journal of Online Biomedical Engineering, vol. 18, no. 3, pp. 101-113, 2022

[19] W. M. Salih, Ahmed T. Sadiq, and Ibraheem Nadher. "Modified CNN-LSTM for Pain Facial Expressions Recognition, " Vol. 29, No. 3, pp. 304-312, 2020.