March - April 2020
ISSN: 0193-4120 Page No. 5218 - 5224

# An Optimal Auto Encoded Deep Neural Network based Intrusion Detection Systems for Mobile ADHOC Networks

Bosco Paul Alapatt[1], Anupama Jims[2], Dr. Felix M Philip[3]
[1,2,3]Assistant Professor.JAIN (Deemed-to-be University), Kochi
p.bosco@jainuniversity.ac.in[1],j.anupama@jainuniversity.ac.in[2], m.felix@jainuniversity.ac.in.[3]

***Article Info***
***Volume 83***
***Page Number: 5218 - 5224***
***Publication Issue:***
***March - April 2020***

***Article History***
***Article Received****: 24 July 2019*
***Revised****: 12 September 2019*
***Accepted****: 15 February 2020*
***Publication****: 27 March 2020*

**Abstract**

Using the application of ad-hoc networks, communication models in this field of wireless networks have been developed. Greater research is performed for mobile nodes in mobile ad hoc networks (MANET). Intrusion Detection Systems (IDS) is considered as a main component of secured system. A major issue in security system is, it is assumed to be inefficient intrusion detection system due to the access of enormous network information. Traditional IDS provides lower detection rate as well as greater negative alarms with maximum processing time. This study provides an effective IDS method for MANET by combining feature selection (FS) based classifier approach model for efficient identification of intruders. For FS, particle swarm optimization (PSO) algorithm is utilized to pick the essential features from accessible ones. The minimized feature has the subset as and is fed to Auto encoded Deep Neural Network (AEDNN) for discovering the availability of hackers. By including PSO before classification process, it would improve the effectiveness of AEDNN. For practical experience, KDD'99 database is deployed in order to validate the projected technique. The end results signify that greater outcome of PSO-AEDNN model is attained across previous IDS in various estimating variables.

**Keywords;** *MANET; PSO; AEDNN; Classification*

## I. INTRODUCTION

Network abnormalities, present in various types of mobile ad hoc network (MANET), attained due to the dynamic characteristics [1]. A variety of causes could be stated for these anomalies, like improper functioning of network equipment, congestion of network and active assault. Intrusion, which is an anomaly target the service reliability and accessibility [2]. Denial of service (DoS) attack is major intrusion that is used in degradation of service provided by particular target for alternate legitimate consumers [3]. DoS, could be applied in many divisions like Blackhole, Grayhole, Wormhole and Flooding [4]. Each exploits various security breaches in network and affects some of the aspects namely traffic flood, connection disruption, blocking admission or system disturbance in wireless systems [5]. Flooding attacks directly mark a network member by the transmission of negative information or control packets. It is depicted in [6], which a flooding kind of attack could minimize the packet delivery around 84%.

User Datagram Protocol (UDP) flooding attack [7], a data flood attack where allocation is overwhelmed through frequent data traffic, using greater bit rate and usual packet size. This is possible when UDP is no connected with any protocol and without any kind of flow control. Intrusion Detection Systems (IDS), developed for detecting and act in opposite to network violations by observation and identification of anomalies. Hence, to make sure the presence and reliability of network service, there is an emergency



*Published by: The Mattingley Publishing Co., Inc.*

March - April 2020
ISSN: 0193-4120 Page No. 5218 - 5224

to contain systems executed and maintained properly.

In recent days, observing method for predicting DoS attacks in Wireless Mesh Networks (WMN) that is presented [8]. Performance of this technique is estimated on the basis of packet delivery range, maximum packet drops and later measures. Proposed IDS eliminates malevolent nodes and maximizes the packet delivery ratio during the reduction of packet drop by combining a priority model within the network. Therefore, presentation of presented model is sampled for static mesh networks as well as the performance of mobile network could not be examined. Fig. 1 offers the taxonomy of the available IDS methods.

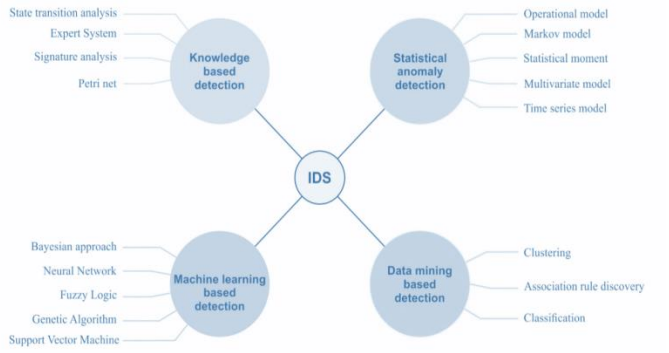


**Fig. 1. Taxonomy of IDS Methods**

New tracking algorithm named as Zone Sampling Based Trace back (ZSBT), developed for tracking malicious nodes present in MANET [9]. In this method, each node contain zone ID within the packet using definite possibility in prior to send the packet. Once packets are received, affected node traces DoS attack again to the initial point for constructing a way among attacker. Accuracy of ZSBT techniques require enhancement while zone associated with more number of nodes. In those cases, identifying malicious nodes would not be accurate. Using SVM for the prediction of DoS attacks are explained in [10]. The outcome of the projected model is evaluated practically and represents the presented SVM based detection method attains maximum or optimal detection accuracy. Hence, in enhancing network performance using suggested technique which not yet analyzed.

Proactive detecting mechanism introduced in [11] for Distributed DoS (DDoS) attacks with decreased computation difficulty. This model is used in detection methodologies of every received packet for extracting suspicious data packets while pre-attack stage. Moreover, a detailed learning of routing attacks and counter measures in MANET could be identified in [12]. This paper proposes the survey of IDS by pointing advantages and disadvantage. There is an alternate presented model that deals with DDoS attacks in MANET [13]. Existing solutions depends on technique which assume single attribute from network e.g. hello interval delay, else solution is adaptable for single allocated routing approach. Therefore, an intrusion like DoS or DDoS, higher than one fact of network is influenced, and decisions based on special routing protocol is inefficient with various routing protocols, hence a solution assuming the restrictions must be developed.

Traditional IDS provides lower detection rate as well as greater negative alarms with maximum processing time. This study provides an effective IDS method for MANET by combining feature selection (FS) based classification model for efficient identification of intruders. For FS, particle swarm optimization (PSO) algorithm is utilized to select the vital characters from available characters. The minimized feature has the subset as and is fed to Auto encoded Deep Neural Network (AEDNN) for discovering the availability of hackers. By including PSO before classification process, it would improve the effectiveness of AEDNN. For practical experience, KDD'99 database is deployed in order to validate the projected technique. The end results signify that greater outcome of PSO-AEDNN model is attained across previous IDS in various estimating variables.

## II. PROPOSED METHOD

This study provides an effective IDS method for



Published by: The Mattingley Publishing Co., Inc.

March - April 2020
ISSN: 0193-4120 Page No. 5218 - 5224

MANET by combining FS based classificier approach for efficient identification of intruders. For FS, particle PSO algorithm is utilized to select the essential features from present features. The minimized feature has the subset as and is fed to AEDNN for discovering the availability of hackers

### 2.1. PSO-FS

PSO, developed in the year of 1995 is stimedula from social characteristics like bird flocking and fish schooling. Basic concept of PSO optimization of knowledge through social communication in the population in thoughts of personal and social. It depends on the strategy of each solution could be denoted as particle in swarm. Each particle consist of location in search space, that is described through a vector lp = (lp1, lp2, . . . , lpU), where U is the dimensionality of the search space. These particles transform in order to find search space for identifying optimal decisions. As a result, all particles consist of velocity, that is denoted as vp = (vp1, vp2, . . . , vpU). In these cases, every particle updates their position and based on knowledge and adjacent nodes. Earlier best position of a particle named as personal best pbest, and best position reached through the population known as global best gbest. With the help of pbest and gbest, PSO finds best solutions through velocity and location updates of all particles depend on Eq. (1) and (2).

$$l_{pu}^{z+1} = x_{pu}^{z} + v_{pu}^{z+1} \quad (1)$$

$$v_{pu}^{z+1} = w * v_{pu}^{z} + c_1 * r_{1.} * \left(i_{pu} - l_{pu}^{z}\right) + c_2 * r_{2.} * \left(i_{gu} - l_{pu}^{z}\right) \quad (2)$$

where z represents zth iteration in evolutionary operation, u ∈ U denoted uth dimensions in search space. i_pu and i_gu denotes pbest and gbest in the uth dimension. Velocity is restricted by permanent maximum velocity, vmx, and vz+1 pu∈ [−vmx, vmx]. This technique stop, while predefined state is satisfied, that could be extended fitness value or fixed number of iterations.

### 2.2. Classification

Auto-encoders are the variety of artificial neural network utilized for learning effective information demonstration in an unsupervised approach. Under presented concept, an auto-encoder is utilized by encoding as well as decoding layers which have been trained for decrease the restoration mistake. This included prior data from the training group for efficient learning from the information and give optimal action. This pretrained enables both the information to the present task and before connected tasks for self-organizes the learning scheme for create the learning model in information driven fashion. The features are fed to the auto encoder from the trained database with no labels (unsupervised). A group of compacted and robust features are creating at the last part. The encoder parts of the auto-encoder targets for reduce input information into a small dimensional demonstration and they are a decoder part which recreates input information dependent on the small dimension demonstration created with the encoder.

For a provided training database P={p_1,p_2,⋯,p_m}by m samples, where p_z is an n-dimensional characteristic vector, the encoder will map the input vector p_z for a secret demonstration vector h_z with a deterministic mapping f_θas provided in (3)

$$h_z = f_\theta(p_z) = \sigma(Wp_z + b) \quad (3)$$

where W are the x× x, x are the number of secret units, b are the bias vector, θ are the mapping parameter set θ = {W,b}. σ are sigmoid activation function. The decoder maps reverse the resultant secret illustration h_z for a recreated x-dimensional vector q_z in input space.

$$q_i = g_\theta(h_z) = \sigma(Wh_z + b) \quad (4)$$

The aim of trained to the auto-encoder are to reduce the variation among input and outcome. So, the fault



Published by: The Mattingley Publishing Co., Inc.

March - April 2020
ISSN: 0193-4120 Page No. 5218 - 5224

functions are evaluated with the subsequent equation:

$$E(p,q) = \frac{1}{m}\left\|\sum_{i=1}^{m}(p_z - q_z)\right\|^2 \quad (5)$$

The major objectives are to discover the best parameters for reduce the variation among input and recreated outcome above the entire training set (m).

### 2.1.2. Supervised Classifier model using DNN

The three layer DNN are utilized of a are trained with utilizing the primary auto-encoder, s outcomes as inputs. This task orders are retrained in a supervised approach through the class labels and the input characteristic provided for the classification model. A softmax activation layer is used as the outcome layer. The layer evaluates the failure among the expected values and a true value, also the weights in the network is changed with respect to the failure. The easy softmax layers that are located at the last layer, it could be described as follows:

$$X(c|p) = argmax_{c\epsilon C}\frac{\exp(p_{U-1}W_U + b_U)}{\sum_{k=1}^{Z_C}\exp(p_{U-1}W_k)}, \quad (6)$$

where c are the numbers of class, U are the end layer index, and Z_C represents the class count with usual network link and intrusion. Next to this phase, every layer is adjusts with back-propagation in a supervised path. In the analysis stage, the softmax layer results the possibility of the expected divisions.

Fig. 2 offers the action of the network training method to 100 iterations. In training, extra methods can be used namely failure and batch normalization to keep away from above fitting along with for speedup to trained method. The presented technique attains just about 99% accuracy to the training group in 20 rounds that are 4 times quicker if zero failure and batch normalization be utilized. It permits a decrease in the training times needed, and would be of very important value to growing low delay concepts and training future networks by higher information groups. The presented techniques are summarized here in Algorithm 1.

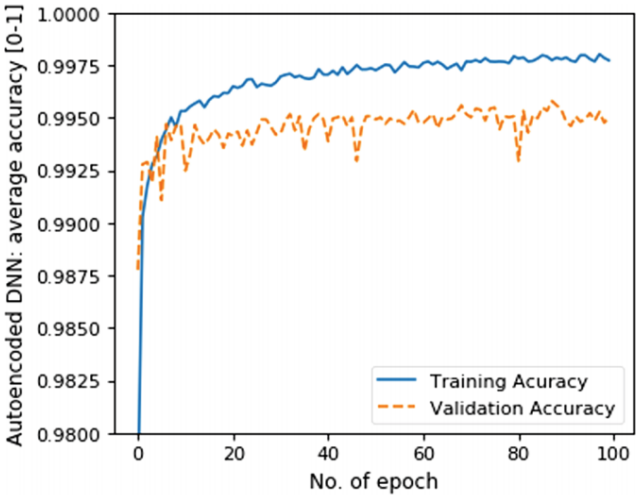


**Fig. 2. Training and validation outcome over epoch count**

| S. No | Feature name | Type | Min value | Max value |
|---|---|---|---|---|
| 1 | duration | Numeric | 0 | 54,451 |
| 2 | Protocol_ type | Symbolic | 0 | 2 |
| 3 | service | Symbolic | 0 | 64 |
| 4 | flag | Symbolic | 0 | 10 |
| 5 | src_bytes | Numeric | 0 | 89,581,520 |
| 6 | dst_bytes | Numeric | 0 | 7,028,652 |
| 7 | land | Boolean | 0 | 1 |
| 8 | wrong_fragment | Numeric | 0 | 3 |
| 9 | urgent | Numeric | 0 | 3 |
| 10 | hot | Numeric | 0 | 101 |
| 11 | num_failed_logins | Numeric | 0 | 4 |
| 12 | logged_in | Boolean | 0 | 1 |
| 13 | num_compromised | Numeric | 0 | 7479 |
| 14 | root_shell | Numeric | 0 | 1 |
| 15 | su_attempted | Numeric | 0 | 2 |
| 16 | num_root | Numeric | 0 | 7468 |
| 17 | num_file_creations | Numeric | 0 | 100 |
| 18 | num_shells | Numeric | 0 | 2 |
| 19 | num_access_files | Numeric | 0 | 9 |
| 20 | num_outbound_cmds | Numeric | 0 | 0 |
| 21 | is_host_login | Boolean | 0 | 1 |
| 22 | is_guest_login | Boolean | 0 | 1 |
| 23 | count | Numeric | 0 | 511 |
| 24 | srv_count | Numeric | 0 | 511 |
| 25 | serror_rate | Numeric | 0.0 | 1.0 |
| 26 | srv_serror_rate | Numeric | 0.0 | 1.0 |
| 27 | rerror_rate | Numeric | 0.0 | 1.0 |
| 28 | srv_rerror_rate | Numeric | 0.0 | 1.0 |
| 29 | same_srv_rate | Numeric | 0.0 | 1.0 |
| 30 | diff_srv_rate | Numeric | 0.0 | 1.0 |
| 31 | srv_diff_host_rate | Numeric | 0.0 | 1.0 |
| 32 | dst_host_count | Numeric | 0 | 255 |
| 33 | dst_host_srv_count | Numeric | 0 | 255 |
| 34 | dst_host_same_srv_rate | Numeric | 0.0 | 1.0 |
| 35 | dst_host_diff_srv_rate | numeric | 0.0 | 1.0 |
| 36 | dst_host_same_src_port_rate | Numeric | 0.0 | 1.0 |
| 37 | dst_host_srv_diff_host_rate | Numeric | 0.0 | 1.0 |
| 38 | dst_host_serror_rate | Numeric | 0.0 | 1.0 |
| 39 | dst_host_srv_serror_rate | Numeric | 0.0 | 1.0 |
| 40 | dst_host_rerror_rate | Numeric | 0.0 | 1.0 |
| 41 | dst_host_srv_rerror_rate | Numeric | 0.0 | 1.0 |

**Fig. 3. Feature Description**



Published by: The Mattingley Publishing Co., Inc.

March - April 2020
ISSN: 0193-4120 Page No. 5218 - 5224

## PERFORMANCE VALIDATION

To authorizing the outcomes of presented technique, KDD Cup 1999 database [14] are utilized. The KDD'99 databases [14, 15] are usually use to the estimate of IDS, includes a total of 125973 instances below 2 classes such as usual (N) and irregularity (A). Besides, the 37 feature is classified into 3 classes' namely basic feature, contents feature and traffic feature. It specifies of the databases is provided in Table 1 and the feature descriptions are provided in Fig. 3.

**Table 1 Dataset Description**

| Dataset | Source | # of instances | # of attributes | # of class | N/A |
|---|---|---|---|---|---|
| IDS | KDDCup 1999 | 132597 | 37 | 2 | 67333/58620 |

**Table 2 FS outcome on IDS Dataset**

| Number of Iteration | Total No. of Features | PSO (1-10 Iteration) | | | Number of Iteration | PSO (11-20 Iteration) | | |
|---|---|---|---|---|---|---|---|---|
| | | Selected Features | Cost | % of Features Reduced | | Selected Features | Cost | % of Features Reduced |
| 1 | 41 | 19 | 0.0020362 | 54 | 11 | 21 | 0.0013089 | 49 |
| 2 | 41 | 19 | 0.0020362 | 54 | 12 | 21 | 0.0013089 | 49 |
| 3 | 41 | 22 | 0.0018826 | 46 | 13 | 21 | 0.0013089 | 49 |
| 4 | 41 | 20 | 0.0015219 | 51 | 14 | 19 | 0.00093985 | 54 |
| 5 | 41 | 20 | 0.0015219 | 51 | 15 | 19 | 0.00093985 | 54 |
| 6 | 41 | 20 | 0.0015219 | 51 | 16 | 19 | 0.00093985 | 54 |
| 7 | 41 | 21 | 0.0013089 | 49 | 17 | 19 | 0.00093985 | 54 |
| 8 | 41 | 21 | 0.0013089 | 49 | 18 | 19 | 0.00093985 | 54 |
| 9 | 41 | 21 | 0.0013089 | 49 | 19 | 19 | 0.00093985 | 54 |
| 10 | 41 | 21 | 0.0013089 | 49 | 20 | 19 | 0.00093985 | 54 |

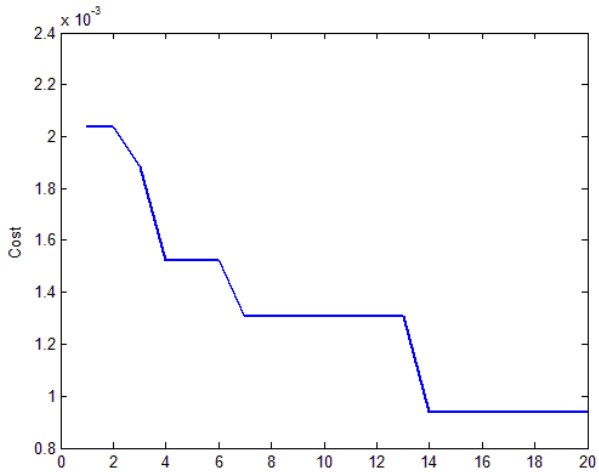


**Fig. 4. Best cost of PSO-FS**

Fig. 4 illustrates the cost analysis of the PSO-FS technique on the tested IDS database.

Table 3 illustrates the relative outcomes of the FS manners with respect to chosen features and optimal cost. As seen in the table, it is noticeable which the presented technique achieves a least optimal cost of 0.00093985.

**Table 3 FS results of PSO algorithm**

| Methods | Best Cost | Chosen Features |
|---|---|---|
| PSO-FS | 0.00093985 | 3,5,8,13,18,20,21,22,23,25,26,28,30,32,33,34,36,38,40 |

Table 4 illustrates the confusion matrix obtained with several classification approaches on the tested



Published by: The Mattingley Publishing Co., Inc.

March - April 2020
ISSN: 0193-4120 Page No. 5218 - 5224

IDS database. Utilizing the values appear in the confusion matrix, arrangement measures would be verified. Table 4, it is exposed which the AEDNN accurately classifies a highest of 66619 and 58471 instances as N and A, correspondingly. However, after the application of PSO, the effectiveness of the AEDNN is developed and the AEDNN accurately classifies a total of 66819 and 58481 instances as N and A, correspondingly. The other techniques namely RBF, LR, and DT illustrate inferior action above the AEDNN and PSO- AEDNN techniques.

**Table 4 Confusion Matrix Intrusion Detection Dataset using Various Classifiers**

| Experts | After FS - AEDNN | | Before FS - AEDNN | | RBFNetwork | | LR | | DT | |
|---|---|---|---|---|---|---|---|---|---|---|
| | N | A | N | A | N | A | N | A | N | A |
| N | 66819 | 524 | 66619 | 724 | 62876 | 4467 | 65540 | 1803 | 64662 | 2701 |
| A | 149 | 58481 | 159 | 58471 | 4443 | 54187 | 1841 | 56789 | 2919 | 55711 |

Table 5 illustrates the applied classifier outcomes in terms of several evaluation parameters. Fig. 5 shows the different comparative outcome classification and their performance on IDS Dataset in terms of dissimilar measures. It is prominent that classification actions are inferior to RBFNetwork. Under FPR and FNR, the values have to least for denote efficient classifier action. The table indicated that advanced value of FPR is achieved with RBFNetwork and DT by the values of 7.61 and 4.62 correspondingly.

**Table 5 Classifier results study on IDS dataset**

| Classifier | FPR | FNR | Sensitivity | Specificity | Accuracy | F-score | Kappa |
|---|---|---|---|---|---|---|---|
| AEDNN | 1.22 | 0.23 | 99.76 | 99.77 | 99.30 | 99.34 | 99.22 |
| RBFNetwork | 7.61 | 6.59 | 93.40 | 92.38 | 92.93 | 93.38 | 85.79 |
| LR | 3.07 | 2.73 | 97.26 | 96.92 | 97.10 | 97.29 | 94.19 |
| Decision Tree | 4.62 | 4.31 | 95.68 | 95.37 | 95.53 | 95.83 | 91.03 |

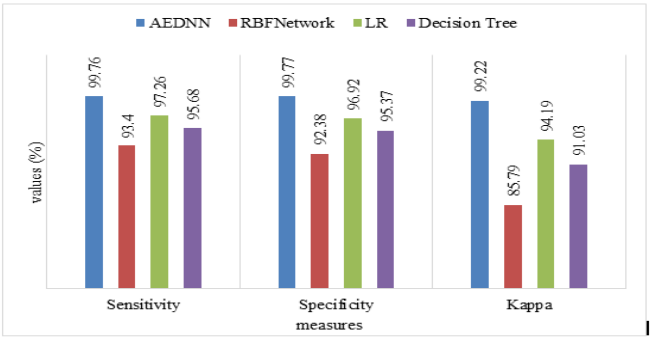


**Fig. 5. Classifier results analysis on IDS dataset in terms of various measures**

**Table 6 Classifier results with and without FS on IDS Dataset**

| Classifier | FPR | FNR | Sensitivity | Specificity | Accuracy | F-score | Kappa |
|---|---|---|---|---|---|---|---|
| AEDNN with FS | 0.89 | 0.21 | 97.87 | 97.91 | 89.47 | 96.39 | 95.33 |
| AEDNN none | 1.22 | 0.23 | 99.76 | 99.77 | 94.30 | 99.34 | 99.22 |

Table 6 gives the classifier outcomes of the presented AEDNN classifier together with the PSO dependent FS task. Fig. 6 illustrates the effect of classification outcomes with utilize of FS process. It is verified from the enhanced FPR of 0.89, FNR of 0.21, sensitivity of 97.87, specificity of 97.91, accuracy of 89.47, F-score of 96.49 and kappa value of 95.93. It is examined that the accurateness achieved with AEDNN before and after PSO is 99.47 and 94 .30 correspondingly. These values verified which the classifier outcome is improved with including PSO in AEDNN.

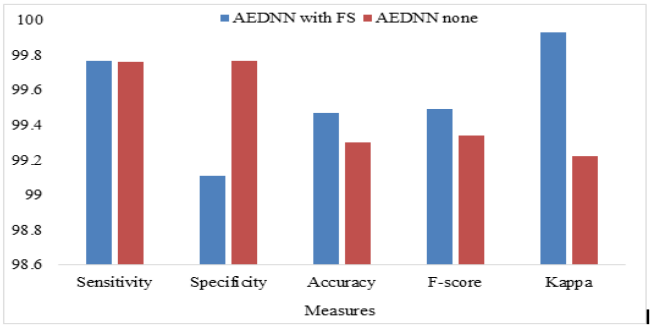


**Fig. 6. Classification results by the use of FS process**



Published by: The Mattingley Publishing Co., Inc.

## III. CONCLUSION

An effective IDS was introduced by this study and a method for MANET by combining FS based classification model for efficient identification of intruders. By including PSO before classification process, it would improve the effectiveness of AEDNN. For practical experience, KDD'99 database is deployed in order to validate the projected technique. The end results signify that greater outcome of PSO-AEDNN model is attained across previous IDS in various estimating variables. From experimental outcome, the accuracy achieved with AEDNN before and after PSO is 89.47 and 94.30 correspondingly. Verifying which the classifier the outcome values have improved with including PSO in AEDNN

## REFERENCES

[1]. Denko, M. K. (2005). Detection and prevention of denial of service (DoS) attacks in mobile ad hoc networks using reputation based incentive scheme. Systemics, Cybernetics and Informatics, 3(4), 1–9.

[2]. Di Pietro, R., Guarino, S., Verde, N. V., & Domingo-Ferrer, J. (2014). Security in wireless ad-hoc networks—A survey. Computer Communications, 51, 1–20. doi:10.1016/j.comcom.2014. 06.003.

[3]. Zargar, S. T., Joshi, J., & Tipper, D. (2013). A survey of defense mechanisms against distributed denial of service (DDOS) flooding attacks. IEEE Communications Surveys and Tutorials, 15(4), 2046–2069. doi:10.1109/SURV.2013.031413.00127.

[4]. Jhaveri, R. H., Patel, S. J., &Jinwala, D. C. (2012). DoS attacks in mobile ad hoc networks: A survey. In 2012 second international conference on advanced computing & communication technologies (pp. 535–541). IEEE. doi:10.1109/ACCT.2012.48

[5]. Chhabra, M., & Gupta, B. B. (2014). An efficient scheme to prevent DDoS flooding attacks in mobile ad-hoc network (MANET). Research Journal of Applied Sciences, Engineering and Technology, 7(10), 2033–2039.

[6]. Desilva, S., &Boppana, R. V. (2005). Mitigating malicious control packet floods in ad hoc networks. In IEEE wireless communications and networking conference, 2005 (Vol. 4, pp. 2112–2117). IEEE.

[7]. Mirkovic, J., Fahmy, S., Reiher, P., Thomas, R., Hussain, A., Schwab, S., &Ko, C. (2006). Measuring impact of DoS attacks. In Proceedings of the DETER community workshop on cyber security experimentation.

[8]. Akilarasu, G., &Shalinie, S. M. (2016). Wormhole-free routing and DoS attack defense in wireless mesh networks. Wireless Networks. doi:10.1007/s11276-016-1240-0.

[9]. Jin, X., Zhang, Y., Pan, Y., & Zhou, Y. (2006). ZSBT: A novel algorithm for tracing DoS attackers in MANETs. EURASIP Journal on Wireless Communications and Networking, 2006(2), 1–9. doi:10.1155/WCN/2006/96157.

[10]. Mukkamala, S., & Sung, A. H. (2003). Detecting denial of service attacks using support vector machines. In The 12th IEEE international conference on fuzzy systems (Vol. 2, pp. 1231–1236). IEEE.