GOF-SLFN- An Intelligent Attack Detection System against Denial of Service (DoS) attacks based on Glow Worm Swarm optimized Single Layer Feed Forward Networks for vehicular Cyber Physical Systems (VCPS)

Rama Mercy Sam Sigamani and Padmavathi Ganapathi

1,2 Department of Computer Science, Avinashilingam Institute for Home Science and Higher Education for Women, Coimbatore, India
1mercyrama@gmail.com, 2padmavathi.avinashilingam@gmail.com

Abstract. Vehicular cyber-physical network use either wireless communications or internet to communicate with each other for an efficient data transfer. Data includes transportation details, safety, mobility and sustainability. However, these communication networks for vehicular transportation are susceptible to different cyber-attacks, which may lead to severe damages or huge casualties in vehicular infrastructures. Hence the intelligent attack detection system needs to be obtaining the lime light of research based on recent machine and deep learning algorithms. In this paper, the GOF-SLFN (Glowworm optimized features for Single-layer feed-forward network) is proposed to detect the attacks among the vehicular cyber physical systems. Since DoS attacks can happen at any layer of OSI Model such as application, network and transport the foremost purpose of the paper is to detect the DoS attacks using the proposed intelligent algorithm. The glowworm algorithm extracted the optimum features based on the probabilistic mechanism and SLFN has been proposed using glowworm to detect the DoS attacks. The proposed system outperformed in detection when compared with artificial neural network, SLFN, Multi-layer Perceptron and random forest. The proposed GOF-SLFN has been again compared with firefly, Bat and Latent Dirichlet Allocation (LDA) and found the proposed intelligent system provided promising results for detection of DoS attacks in VCPS. The proposed system has been tested on the real time scenarios created with SUMO and OMNET++ environment integrated with CIC IDS 2018 datasets. The performance metrics considered were based on accuracy, sensitivity and specificity.

Keywords: Cyber Physical Systems, DoS Attacks, GOF-SLFN, OMNET++, SUMO, transportation.

1. Introduction
A vehicular Information system is a kind of intelligent automobile equipment which provides the drivers and customers with the security, infotainments, environmental conditions and other information services [1]. These kinds of systems consist of body train, power transmission systems, information systems and security systems. Nowadays, with an advent of Internet of things (IoT), vehicular systems have got its more insight in providing the more applications to the customers. Even though vehicular information
system has reached its new dimension, effect of various security vulnerabilities has also reaching its new peak. Many experts, scientists and researchers from the various countries [2] have shown that the security vulnerabilities are common on the vehicles which have adverse effect on authentication, communication and even accident damages. Hence the research on vehicular vulnerabilities is considered to be more important for maintaining the social stability.

Machine learning and Deep learning are playing a very important role in the classification and prediction of the data. To design, an intelligent intrusion system we need the most powerful algorithm to detect and predict the attacks in accordance to take its countermeasures. Several techniques such as “Artificial Neural Networks (ANN), Support Vector Machine (SVM), and Ada boost Classifier” were used for designing an intelligent intrusion system, but detection and measurement need improvisation. Nowadays better machine learning algorithms are replaced by the deep learning algorithms for better detection [1], Since a lot of samples are required for the deep learning framework, machine learning attracts more researchers in dealing with small samples for designing an intelligent intrusion detection system. However, the machine learning based intrusion systems needs more lime light in terms of accuracy and time complexity.

The paper focuses on the implementation of most powerful single feed forward learning algorithm integrated with the Glow worm optimization to detect the different attacks in vehicular networks. The proposed system consists of three different stages such as Data collection, Feature Extraction, Feature Selection and Prediction of attacks. The real time vehicular cyber physical networks are simulated by integrating the SUMO in OMNET Environment and tested with the proposed algorithms on selection of appropriate features thus enabling the better detection of attacks based on the measure of detection accuracy. Moreover, the paper also elaborates the attack detection of the proposed and the existing machine learning algorithms and highlighted the analysed outcome of detection of attacks on comparison.

The organization of the paper is as follows: Section 2 presented the literature study undergone for VANET and its security techniques. Section-3 deals with overview of Uni-layer feed-forward learning machines and Glow worm algorithms. The working methodology such as data collection unit, feature selector and extractor, classifier is detailed in Section-4. Section -5 deals with the experimental design, performance evaluation with comparative analysis between the different learning algorithms. Finally, conclusion is presented in Section-6.

2. Literature Survey

Paul Darby described Decentralized Security Exchange (DSE) to proficiently bolster digital physical security for vehicles, including any electric, self-governing or traditional vehicle having a CAN transport. The exhibition of DSE for different degrees of theoretical registering replication forcefulness is dissected. The significance of the DSE answer for vehicles, particularly during debacle situations is clarified, similar to its pertinence to open trust inefficient power vitality advances.

Huangmiao CHEN dissected security vulnerabilities, dangers and uncommon security prerequisites of the present vehicle data framework. This framework includes data resources in-vehicle framework, divides vehicle data framework into two classes/levels: family and business, and characterizes target and necessity of security assurance for two sorts of vehicle data frameworks, separately. At last, a progression of doable assessment strategies and instruments are exhibited for assessment practice. A major commitment of this paper is to investigate characterized security assurance assessment for the vehicle data framework and tops off the hole of assessing security condition of car data framework everywhere throughout the world [3].

Simona Gifei underlined the significance of managing in an integrative way with security and wellbeing guidelines, meaning to blend a rational procedure for the advancement of self-sufficient vehicles. Reciprocal, it is emphasized the significant coordinating procedure to guarantee intentional ranges for cyber security dangers. The creators propose such a unitary idea for creating self-governing vehicles by coordinating quality, wellbeing and (cyber) security into one framework, called Quality Safety Cyber Security Integrated Management System (QSCSIMS). It displayed the framework and a a numerical model of the related procedures for the standard-based design. The performance metrics such as
improvement of procedures, diminishing of waste, lower costs, protected and secure frameworks lastly, fulfilled clients [4].

Madhusudan Singh examined the accommodate security prerequisites designing to give digital security in IV. To satisfy the proposed goal, objective demonstrating manner of RE, the Knowledge Acquisition in Automated Specification (KAOS) Model methodology utilized for the design of utilizing Objective instrument locating the accommodating prerequisites. Self-compromise is gained by five structure squares, for example, Monitor, Analyze, Plan, Execute and Knowledge for example [MAPE-K] circle engineering, which provided the accommodating abilities to propose accommodating prerequisites of digital security in [5].

Pero Škorput described the malicious attacks and its manifestation on vehicles connected in Cooperative ITS environment. “Public Key Certification Authority Model in Cooperative ITS” model was proposed that lowered the odds of malicious malware attacks with predefined basic set of decisions. The divided five level decisions are for the processing of the security solution in the environment. The Cooperative ITS has a varied challenge in ensuring safety and security due to dissimilar transport modes. The literature study on securing connected vehicles revealed that this kind of environment leads to increase in the harmful rate and fatality rate in transportation when attacked than in other traffic domains. The various intentions both harmless and malicious of attackers in the cyber domain are differentiated as they reflect in the injury and fatalness in large for the road transportation [6].

Muhammad Shafique presented the security threats and their respective threat models in the layers of CPS and identified the relevant research challenges for the development of secure CPS. The challenges identified are addressed with a comparison of the state-of-the-art static and adaptive techniques and analyzed for detection and prevention with associated limitations. This paper further discussed the security techniques against characterized attacks on CPS layers with open research problems in developing the intelligent security measures using machine learning algorithms for CPS. In addition, the paper provided an outlined view of on-going project for securing CPS and the research problems and its motivational analysis aspects were discussed [7].

3. Glow-Worm Swarm Optimization Algorithm

Krishna et.al proposed this swarm based intelligence algorithm for optimizing the multi-model problems. Glow-worm (GLW) swarm optimization technique is adopted in many recent applications for minimizing the search time of optimum to improve the objective function. Likewise, in this article, we adopted this swarm algorithm for attack detection system in vehicular cyber physical systems. Basically glow-worm optimization technique is adopted from natural species of glowworms. GLW is developed using its attraction factor called “luciferin”. Interaction between glow-worms are highly depends on the luciferin factor.

The proposed model initiated with development of fitness function and developed the GLW algorithm. The objection or fitness function is to detect the various attacks in the vehicular systems. The targeted attack in this paper is “DDOS- Distributed Denial of Service” includes diverse modules such as volume attacks, application layer attacks etc. GLW is highly utilized for these attacks detection in the specified location to enhance the vehicular system efficiency.

3.1. GLW Stages

GLW initially starts with random value in the search space to detect the optimum value based on the defined fitness function. The glow-worm algorithm involves three stages in each iteration to detect the local optimum value in the current space. Three stages are given below.

- Glow-worm attraction factor update stage
- Glow-worm movement stage
- Glow-worm neighbourhood stage

**Glow-worm Attraction Factor Update Stage:**

In the GLW algorithm, attraction factor is “luciferin” which produces the light enzyme on its own. Based on this attraction factor, each glow-worm interacts with neighbor glow-worms. The capability of
luciferase enzyme is directly proportional to the present location of glowworm in the given search space. In this stage, it detects the local optimum value in the given search area rather than global value. Likewise, each glowworm attracted each other based on the highest luciferin values and updated with the current value. Similarly, the glowworm updates its attraction factor values nearer the optimum. The key rule of the attraction factor is given in the below equation 1.

\[ F_j(S + 1) = (1 - \delta)F_j(S) + \omega O_j(S + 1) \]  

where \( \delta \) is the luciferin decay constant \([0, 1]\) and \( \omega \) denotes the luciferin enhancement constant which is set as 0.6. The objective function is \( O_j(S+1) \) at ‘j’ location at sample time ‘S’.

**Glow-worm Movement Stage**

In this second stage, “probabilistic mechanisms” plays a major role in glowworm technique. Naturally, glowworm attracts its neighbor based on the above mechanism. It checks the brightness of its own with its neighbor and attracted each other. Likewise, it moves entirely in the search space and detected the nearer optimum value. Fig.2 describes the probabilistic mechanism in detail with six glowworms. The probability movement of each glowworm ‘i to j’is given below.

\[ \varphi_j(S) = l_j(S) - l_i(S)/\sum_{k=M_i(S)} l_k(S) - l_i(S) \]  

where \( j \in M_i(S) \)

\[ M_i(S) = \{ j; d_{ij} < r_d^i(S); \} \]  

‘S’ denotes the step index and \( d_{ij} \) represents the Euclidean distance. \( M_i(S) \) represents that movement towards the neighbour j from i by computing the Euclidean distance between i and j based on the luminescence level associated with glowworm j at time t.

Discrete-time movements are given below.

\[ G_i(S) = G_i(S) + \rho(G_{ij}(S) - G_i(S))/\|G_i(S) - G_i(S)\| \]  

**Glowworm Neighborhood Stage**

Normally, local optimum values are detected in the previous stages. In this phase, the local optimum values are ignored and the global optimum values are selected from the given workspace. It detects the multiple sensor locations and continues the attraction process in the neighborhood range. Multiple peaks are identified by varying the sensor range. For this purpose, glowworm agent ‘i’ is within the local-decision domain with dynamic radial range \( 0 < r_d^i \leq r_s^i \). The enhancement movement is obtained using equation 5.

\[ r_d^i(S + 1) = min\{r_2, max\{0, r_d^i(S) + \beta(S_t - |M_i(S)|)\}\} \]
Hence the optimization technique is used for the best feature selection in order to get the best features that enable to detect attacks based on their change in their values.

3.2. UNI-Layer ELM Network

The proposed uni-layer neural network follows the “ELM-extreme learning machine model”. As per [12] [13], ELM provides high speed, exactness, preparing velocity, speculation and approximation functions. In this paper, we developed this uni-layer elm network for detecting DDoS attacks in the vehicular CPS. Each node in the hidden layer process the various vehicles input features and detects the output layer. The novel of the proposed network is automatic tuning is not required for this network. Hidden nodes need not tuning. The activation function utilized in the proposed model is sigmoid function. Let ‘L’ denotes the hidden neurons and output layer is denoted by ‘z’.

The algorithm of Uni-layer ELM is as follows:

Initial Phase
Input: The arrived data, a kernel function $k(x_i, x_j)$ and a regularization parameter $C$.

Output: $\varphi_i$
1. $\Omega_i = (C^{-1} + \Delta ELM - I)^{-1}$
2. $\varphi_i = \Omega_i \cdot T_i$

Sequential Phase
Input: The $(i+1)^{th}$ sampling data

Output: $\varphi_{i+1}$

---

**Figure 1. Glowworm Neighborhood Stage**
4. Proposed Architecture
The proposed architecture consists of three different phases such as Data collection unit, feature Extractor and Selector using Glow worm optimizer and Single layer feed forward Networks. The working methodology of the three different phases is detailed in this section.

4.1. Data Collection Unit
The real time scenario has been created with the SUMO software. The position of the vehicles at a particular time $t$ on the road is computed using a microscopic traffic based on vehicles and road characteristics. These positions are used to show vehicles on a graphical user interface (GUI) or written in a file (dump file). The different real time scenarios for the vehicular systems are created as shown in Fig. 2 and Fig. 3.

![Real Time Scenario for the Vehicles cyber systems created by the SUMO-OMNET Environment](image)

**Figure 2.** Real Time Scenario for the Vehicles cyber systems created by the SUMO-OMNET Environment
Figure 3. Real time Road Scenario with the Four Lane /Two Lane Road System using SUMO-OMNET Environment

The input data are the initial positions, vehicle characteristics (acceleration, maximum speed), road network, directions, position of destination, speed limits, etc. SUMO [15] a simulator with a feature to support car-following model (issue of [16-19]) used in this paper creates a road side scenario. These are simulated as the nodes in an OMNET ++ environment. The list of parameters which are created by SUMO are listed in Table I.

| S.NO | List of parameters | Specifications         |
|------|--------------------|------------------------|
| 01   | No of vehicles     | 100                    |
| 02   | Speed              | 35-40 km/hr            |
| 03   | Direction          | Bi directional         |
| 04   | Type of roads      | Two-lane /Four Lane Roads |
| 05   | Network used       | IPv6                   |
| 06   | No of attacks used | 02                     |

Table I shows the different parameters collected in the SUMO Interfaces. After converting as the nodes using OMNET++ Environment, different features such as no of TCP packets transmitted, No of packets received, Signal Strength, latency, Speed of the vehicles, Direction, throughput, time stamp, Input Message ID and layer ID were calculated manually. The calculated features are listed in Table II.

4.2. Feature Selector and Extractor

As discussed above, various features were calculated from the network scenario to detect the various attacks. Since the number of features is more, it may cause the instability in the classifier which results in inaccurate predictions. Hence the optimization technique is used for the best feature selection in order to get the performance. The fitness function for calculating the best features is given as in equation 6.

| S.NO | List of parameters                          | Specifications     |
|------|--------------------------------------------|--------------------|
| 01   | No of TCP packets Transmitted              | 8 bytes            |
| 02   | No of TCP Packets Received                 | 8 bytes            |
| 03   | Speed of the vehicles                      | 35-40 km/hr        |
| 04   | Signal Strength                            | -10 to 25 dbm      |
where \( WB \) is the actual no of features used, \( G_i \) is Cost function \( F_i \) is No of feature to be selected. From the 10 features collected from the real time scenario, 05 features were optimized as the best features for the high accurate classification. The obtained five features are taken as the inputs for the SLFN for classification and prediction of attacks. The labeled features used for the prediction of attacks are listed in table III.

4.3. SLFN Classifier
The labeled features are then feed to the SLFN classifier which consists of seven input layers and three output layers which depend on number of attacks. The proposed classifier classifies the different attacks based on the above equation 6. The pseudo code of the proposed classifier is as follows

\[
Fitness\_Function = W_B + \left \{ i = 1 \sum_n G_i X F_i \right \}^{-1}
\]

(6)

5. Results and Discussions

5.1. Experimental Setup
As discussed in above section-II, SUMO integrated with the OMNET has been used for the real time data collection under normal conditions. To identify the different attacks, CIC-IDC2018 datasets were used as the reference in the real time scenario created. Nearly 1500 data were collected and used for the experimenting the proposed algorithm.

5.2. Performance Evaluation
The Glowworm features which are extracted from the datasets are used for training and testing process. For evaluation, the data collected are segregated as training and test data with proportions of 70% and 30% respectively. The evaluation is carried out for the different glow worm datasets with the performance parameters as in equations 7, 8 and 9.

\[
Accuracy = \frac{DR}{TN} \times 100
\]

(7)
Sensitivity = \frac{TP}{TP+TN} \times 100 \quad (8)

Specificity = \frac{TN}{(TP+TN)} \times 100 \quad (9)

Where TP and TN represents True Positive and True Negative values and DR & TNI represents the Number of Detected Results and Total number of Iterations. The proposed GOF-SLFN algorithm has been evaluated by different cases based on the performance.

**Accuracy Evaluation**

For accuracy evaluation, the proposed algorithm has been executed for the 100 trials and mean of the results has been considered as final accuracy for the classification of different attacks in the transportation vehicular networks. The accuracy has been calculated for classification of different attacks. The accuracy of the proposed algorithm has been evaluated using the different learning kernels are shown in the Table 4.

**Table 3.** List of Labelled Features used by the Proposed Architecture for Classification of different attacks

| No of TCP packets Transmitted | No of TCP packets Received | Throughput | Latency (ms) | Time of arrival to OBU (ms) | LayerID | Msg ID | Label | Label Details |
|-------------------------------|----------------------------|------------|--------------|----------------------------|---------|--------|-------|----------------|
| 5                             | 5                          | 48         | 0.7          | 0.45                       | 186     | 457    | 0     | Normal         |
| 5                             | 5                          | 62         | 0.8          | 0.458                      | 174     | 427    | 0     | Normal         |
| 5                             | 5                          | 25         | 0.3          | 0.459                      | 60      | 138    | 0     | Normal         |
| 5                             | 5                          | 60         | 0.5          | 0.45                       | 66      | 153    | 0     | Normal         |
| 5                             | 5                          | 46         | 0            | 0.45                       | 30      | 63     | 0     | Normal         |
| 5                             | 5                          | 49         | 0.1          | 0.45                       | 42      | 93     | 0     | Normal         |
| 5                             | 5                          | 8          | 3.2          | 0.78                       | 36      | 78     | 2     | Botnet         |
| 5                             | 5                          | 29         | 4            | 0.45                       | 36      | 525    | 0     | Normal         |
| 5                             | 5                          | 46         | 0            | 0.457                      | 84      | 547    | 0     | Normal         |
| 5                             | 0                          | 7          | 5            | 0.88                       | 101     | 496    | 1     | DOS            |
| 5                             | 0                          | 9          | 5.6          | 0.90                       | 107     | 498    | 1     | DOS            |
| 5                             | 0                          | 5          | 10           | 0.92                       | 113     | 500    | 1     | DOS            |
| 5                             | 0                          | 7          | 12           | 0.94                       | 119     | 502    | 1     | DOS            |
| 5                             | 0                          | 7          | 17           | 0.96                       | 125     | 504    | 1     | DOS            |
| 5                             | 0                          | 9          | 25           | 0.98                       | 131     | 506    | 1     | DOS            |
| 5                             | 0                          | 5          | 6.7          | 0.95                       | 137     | 514    | 1     | DOS            |
| 5                             | 0                          | 64         | 0.2          | 0.50                       | 66      | 153    | 0     | Normal         |

**Table 4.** Accuracy Comparison for different learning function used in Proposed Algorithm

| S.No | Dataset details | Learning Kernel | Training Accuracy | Testing Accuracy |
|------|----------------|-----------------|------------------|-----------------|
| 01   | Five Feature Dataset | Sigmoid | 95.5% | 95.4% |
|      |                 | Sine        | 95.0% | 94.5% |
|      |                 | Tanh        | 95.0% | 94.5% |
From TABLE 4, it is evident that the accuracy of 94.5% obtained when the sigmoidal function is adopted for the proposed algorithm for CIC IDC datasets is maximum. Again the accuracy of the proposed GOF-SLFN along with the Sigmoidal learning function is evaluated with randomly chosen hidden neurons are shown in Table 5.

TABLE 5 clearly shows that the sigmoidal learning along with 75 neurons has a maximum accuracy of 95.5% in the classification of different attacks of vehicular cyber physical systems. The highest accuracy obtained from GOF-SLFN has been compared with other learning algorithms for the evaluation of the performance based on the classification of attacks. The different scenarios of attacks have been considered for comparing the proposed algorithm with other existing learning algorithms.

**Table 5. Accuracy Comparison for different neurons used in gof-slnf algorithm**

| Sl.No | Dataset details     | No of neurons | Training Accuracy | Testing Accuracy |
|-------|---------------------|---------------|-------------------|------------------|
| 01    | Five Feature Dataset| 10            | 93.5%             | 93.0%            |
|       |                     | 20            | 93.5%             | 91.5%            |
|       |                     | 50            | 92.5%             | 92.5%            |
|       |                     | 75            | 95.5%             | 94.5%            |
|       |                     | 100           | 91.5%             | 92.4%            |
|       |                     | 150           | 92.4%             | 91.5%            |
|       |                     | 200           | 91.5%             | 92.5%            |

5.3. Scenario-I Analysis

In the first scenario, DoS attacks were considered for the classification and different comparative analysis are shown in following Fig. 4.

![Figure 4. Training Accuracy Analysis for the different Algorithms in classifying/predicting the DoS Attacks](image)

![Figure 5. Testing Accuracy Analysis for the different Algorithms in classifying/predicting the DoS Attacks](image)
Fig. 4 and Fig. 5 clearly shows training and testing accuracy of the proposed algorithm as 95.5% when compared with the other algorithms such as Multilayer perceptrons (MLP), Artificial neural networks (ANN), and Random Forest (RF).

**Sensitivity and Specificity Analysis**

Again the sensitivity and specificity has been calculated and compared with the learning algorithms in which the proposed algorithm outperforms the other existing algorithms. Fig.6 and Fig. 7 shows this analysis made.

![Sensitivity Analysis](image)

**Figure 6.** Sensitivity Analysis for the different Algorithms in classifying/predicting the DoS Attacks

![Specificity Analysis](image)

**Figure 7.** Selectivity Analysis for the different Algorithms in classifying/predicting the DoS Attacks

### 5.4. Scenario-II Analysis

In the second scenario, Bomb net attacks were considered for the classification and evaluation. The comparative analysis between the proposed algorithm are depicted in following TABLE 6.

| Attack           | Algorithm | Accuracy | Sensitivity | Specificity |
|------------------|-----------|----------|-------------|-------------|
| Botnet Attacks   | ANN       | 88.5%    | 88.0%       | 89.0%       | 89.0%       |
|                  | RF        | 92%      | 91.5%       | 92%         | 91.5%       |
|                  | MLP       | 91%      | 90%         | 91%         | 90.5%       |
|                  | Proposed algorithm GOF-SLFN | 95.5% | 95.0% | 94.0% | 95.0% |
From the table it is clear that performance of proposed algorithm has outperformed the existing learning algorithms in terms of accuracy, sensitivity and specificity.

5.5. Time Analysis
The training and testing time has been calculated for the proposed GOF-SLFN and compared with the other existing algorithms. The Table 7 shows the comparative analysis of training time and testing time for different networks with respective to different attacks.

Table 7. Comparing Training Time of Proposed GOF-SLFN Model with the existing algorithms in detection of attacks

| Types of Attacks | GOF-SLFN | SLFN | MLP | RF | ANN |
|------------------|----------|------|-----|----|-----|
| DoS attacks      | 0.233    | 0.345| 0.1269| 0.298| 4.56 |
| BotNet attacks   | 0.231    | 0.3300| 0.1278| 0.288| 4.67 |

Table 8. Comparing Testing Time of Proposed GOF-SLFN Model with the existing algorithms in detection of attacks

| Types of Attacks | GOF-SLFN | SLFN | MLP | RF | ANN |
|------------------|----------|------|-----|----|-----|
| DoS attacks      | 0.109    | 0.117| 0.118|    | 2.39 |
| BotNet attacks   | 0.112    | 0.111| 0.121| 0.121| 2.78 |

From the above tables 7 & 8, time complexity is also reduced in the proposed algorithm on comparison with the machine learning algorithms in detection of different attacks in real time vehicular scenario. Table 9 depicts the comparative analysis of the proposed algorithm with different optimization algorithms namely, firefly, Bat and LDA. From the table, the proposed algorithm provides promising detection accuracy than other optimization algorithms.

Table 9. Comparing Testing Time of Proposed GOF-SLFN Model with the existing algorithms in detection of attacks

| S.No | Algorithms | Performance Metrics | DoS Attacks | Botnet Attacks |
|------|------------|---------------------|-------------|----------------|
| 1    | Swarmfly-SLFN | Training Accuracy | 87.5% | 86.45% |
|      |            | Testing Accuracy   | 87.0% | 86.0% |
|      |            | Sensitivity        | 86.0% | 84.0% |
|      |            | Specificity        | 85.0% | 83.0% |
|      |            | Training Accuracy  | 93%   | 92%  |
|      |            | Testing Accuracy   | 92.5% | 91.0% |
|      |            | Sensitivity        | 92%   | 91%  |
|      |            | Specificity        | 91.5% | 90.5% |
| 2    | BAT-SLFN   | Training Accuracy  | 94%   | 94%  |
|      |            | Testing Accuracy   | 93%   | 93%  |
| 3    | LDA-SLFN   | Training Accuracy  | 94%   | 94%  |
|      |            | Testing Accuracy   | 93%   | 93%  |
6. Conclusion

The proposed GOF-SLFN algorithm has been designed based on the glowworm optimizer integrated with Single layer feed forward networks with 75 neurons for the detection of different DoS attacks. The performance of the proposed algorithm has better accuracy in detection, better sensitivity and selectivity than the existing machine learning algorithm. The proposed classifier seems to be more intelligent in detection of the attacks and finds its application in vehicular cyber physical systems. The algorithm can be improvised by testing with the more number of attacks since the paper deals with the only two different types of attacks. The implementation of bio-inspired algorithms and deep learning algorithms will improvise the accuracy of detecting the different attacks. The future scope of this work can be considered based on the implementation of deep learning algorithms which will improvise the accuracy of detecting the different attacks.

References

[1] Syed J, Gardezi S, Awais M, Faye I and Meriaudeau F 2017 Mammogram Classification using Deep learning features IEEE Int. Conf. on Signal and Image Processing Applications (ICSIPA).
[2] Darby P and Gottumukkala R 2019 Decentralized Computing Techniques in Support of Cyber-Physical Security for Electric and Autonomous Vehicles IEEE Green Technologies Conf. (GreenTech) 1-5.
[3] Chen H, Chen X, Fan L and Chen C 2015 Classified security protection evaluation for vehicle information system Int. Conf. on Cyber Security of Smart Cities, Industrial Control System and Communications (SSIC) 1-6.
[4] Gifei S and Salceanu A 2017 Integrated Management System for quality, safety and security in developing autonomous vehicles 10th Int. Symp. on Advanced Topics in Electrical Engineering (ATEEE) 673-676.
[5] Singh M and Kim S 2017 Reconcile security requirements for intelligent vehicles 17th Int. Conf. on Control, Automation and Systems (ICCAS) 1646-1651.
[6] Kim H, Ju B and Na J 2018 An Access Control Method for Vehicle Management System Int. Conf. on Information and Communication Technology Convergence (ICTC) 949-952.
[7] Mansfield K, Eveleigh T, Holzer TH and Sarkani S 2013 Unmanned aerial vehicle smart device ground control station cyber security threat model IEEE Int. Conf. on Technologies for Homeland Security (HST) 722-728.
[8] Jin PJ, Zhang G, Walton CM, Jiang X and Singh A 2013 Analyzing the impact of false-accident cyber-attacks on traffic flow stability in connected vehicle environment Int. Conf. on Connected Vehicles and Expo (ICCVE) 616-621.
[9] Javaid A, Sun W, Devabhaktuni VK and Alam M 2012 Cyber security threat analysis and modeling of an unmanned aerial vehicle system IEEE Conf. on Technologies for Homeland Security (HST) 585-590.
[10] Škorput P, Vojvodić H and Mandžuka S 2017 Cyber security in cooperative intelligent transportation systems Int. Symp. ELMAR 35-38.
[11] Shafique M, Khalid F and Rehman S 2018 Intelligent Security Measures for Smart Cyber Physical Systems 21st Euromicro Conf. on Digital System Design (DSD) 280-287.
[12] Huang GB, Zhu QY and Siew CK 2006 Extreme learning machine: theory and applications Neurocomputing 70 489-501
[13] Lian C, Zeng Z, Yao W and Tang H 2013 Displacement prediction of landslide based on psogsa-elm with mixed kernel Sixth Int. Conf. on In Advanced Computational Intelligence (ICACI) 52-57.

[14] Wang B, Huang S, Qiu J Liu Y and Wang G 2015 Parallel online sequential extreme learning machine based on MapReduce Neurocomputing 149 224-232.

[15] Lu S and Lu Z 2016 A pathological brain detection system based on kernel-based ELM Multimed Tool Appl. 1-14.

[16] Krauss S 1998 Microscopic modeling of traffic flow: Investigation of collision free vehicle dynamics.

[17] Wagner P and Lashevsky I 2003 Empirical basis for car-following theory development.

[18] Kerner BS 2009 Introduction to modern traffic flow theory and control: the long road to three-phase traffic theory Springer Science & Business Media.

[19] Treiber M, Ansgar H and Dirk H 2000 Congested traffic states in empirical observations and microscopic simulations Physical review E. 62 1805.