International Journal of Computing and Digital Systems
ISSN (2210-142X)
Int. J. Com. Dig. Sys. 12, No.1 (Nov-2022)

https://dx.doi.org/10.12785/ijcds/1201105

P2PCPM: Point to Point Critical Path Monitoring Based Denial of Service Attack Detection for Vehicular Communication Network Resource Management

Vartika Agarwal[1] **and Sachin Sharma**[1]

[1]*Department of Computer Science and Engineering, Graphic Era Deemed to be University, Dehradun,India*

Received 31 Dec. 2021, Revised 7 Sep. 2022, Accepted 31 Oct. 2022, Published 30 Nov. 2022

Abstract: Various types of security attacks are normal in vehicular communication networks. The current study uses a support vector machine to implement a Point to Point Critical Path Monitoring (P2PCPM) based Denial of Service (DOS) Attack detection technique for Vehicular Communication Network (VCN) resource management. Greatest quality of P2PCPM is that it eliminates attacked nodes from the network for the smooth process of vehicular communication. This scheme works well in terms of accuracy as well as attack detection rate. The whole simulation is made and tried by utilizing MATLAB Software. Simulation result shows 99% accuracy in case of security attack detection as well as reduced training and testing error upto 2%. Experimental results indicate that this scheme has a great efficiency and works well up to 1000 nodes, which is the limitation of current implementation. In future, simulation test may be done for unlimited nodes using similar or other techniques of attack detection.

Keywords: Denial of Service (DOS), Distributed Denial of Service (DDOS), Point to point Critical Path Monitoring (P2PCPM), Support Vector Machine (SVM),Vehicular Communication Network (VCN)

1. Introduction

VCN is a network which establish communication between different vehicles. Sensors, transmitters and other resources act as medium of communication between vehicles. Such resources have power to share message about traffic and any other emergency. Security attacks such as Spyware, Worms and DOS disrupt this network [1]. Identification of such types of attack is required for smooth working of vehicular communication. Sometimes message or information may be delay because of such attacks. This delay will result in an accident, and a significant amount of time will be wasted in traffic. We use DOS attack detection technique for vehicular communication network which is based on P2PCPM. DOS is an unauthorised attempt to crash the vehicular communication network and making it difficult to reach to its actual users [2]. In this research, a vehicle is represented by sensor node. Radio transmissions can be used to communicate between sensor nodes. We create a training model to train the Support Vector Machine (SVM) learning model, and then we test it on real-world data to find the attacked nodes and calculate both the training and testing errors. DOS attacks are generated by any person, organisation for crash the network. Such unauthorised users send same information again and again by using the network resources. Due to this unauthorised activity, actual users unable to access the network. Such attacks can be mostly found in network and transport layer. There are two kinds of DOS attack – Jamming as well as Tampering. In Jamming, legitimate user (attacker) tries to break the network. . In Tampering, attackers target the sensor nodes. E-Commerce websites, VCN, or any online service provider are the main target of attackers. For preventing DOS attacks we generate a strong vehicular communication network and detect DOS attacked node and remove it from the network. The importance of DOS detection are as follows [18]:
DOS attack is responsible for slow down the communication between vehicles. So for the faster response, it is needed to recognize vehicles which are responsible for DOS attack.
DOS damage network resources and generate a lot of fake signals. The result of the fake signal is authorized vehicles are unable to communicate. DOS hangs the complete system and stops the whole communication process. DOS attacks are launched by an attacker. They generate malicious packets and increase the network load.
Main contribution in this paper are as follows:
Generate a P2PCPM based vehicular communication network. Detecting attacked nodes from the network Eliminate such kind of nodes and repeat the process until all attacked nodes are not identified. Ensure smooth work of the network vehicular communication process. The research organization is done as follows: Section II depicts the related work in this research. Section III present method and implementation of proposed system. Section IV discuss about performance and result of this simulation. Section V

E-mail address: vartikaagarwal2015@gmail.com, sachin.cse@geu.ac.in,

conclude the work with summary and highlight the future scope of proposed system.

2. Literature Review

Several experts have worked for the security attacks in last two decades(Table I). In 2017, Myeongsu Kim propose mechanism of security attack detection in a software defined network. Experimental result validate that this scheme works well for identifying types of cyber attack [1]. In 2017, Narmeen Zakaria Bawany, propose novel structure for security attack identification in SDN. This framework is beneficial for smart cities where there a huge chances of such types of attacks [2] . In 2017, Tasnuva reviewed about techniques of security attack detection and prevention. They highlight the impact of techniques, challenges as well as experimental model used by different authors for such research [3]. In 2017, Mohamed Idhammad design deep learning based method of DOS identification. This technique has a great accuracy and it outperform other detection techniques in terms of security [4]. In 2017, Chuan long propose intrusion detection system by using deep learning. It has a great accuracy rate and better result in comparison of other security techniques [5]. In 2018, Lei SU introduced a supervisory model for detecting the attacker behavior. They analyze the performance of this technique by using attack success rate and packet reception rate [6]. In 2018, Shailendra Rathore use supervised machine learning algorithm for identifying attacked nodes as well as normal nodes. It has 86% accuracy and achieve better performances then the other security attack detection framework [7].In 2018, Julio Navarro explain mechanism about how attackers attack on the network and break the security features. They discuss about how to recognize such types of cyber attack [8].In 2018, Yunsheng Fu propose attack detection model based on LSTM and RNN .They use Bayesian theorem for train the neural network . Experimental result validate that it has 80% accuracy and less network drop rate [9].In 2018, Gao Liu review about various security attacks , previous work on security measures and point out future research direction [10].In 2019, Francisco present DOS attack detection model It has a great accuracy, high precision as well as low false alarm rate [11]. In 2019, Gradient descent algorithm are proposed by Gayathri for identification of security attacks. This algorithm has achieved 97% accuracy which is far better than other intrusion detection system [12]. In 2020, Bombang present security attack detection model which is based on machine learning. It has a great accuracy, better throughput as well as faster response time. [13]. In 2020, deep neural network was presented by Sumitha for security attack detection. It has less network drop rate as well as great efficiency [14]. In 2020, novel tensor based structure are proposed by Joao Palo for security attack identification using machine learning concept.This framework provides better throughput and achieves 95% accurate results [15]. In 2020, Swathi use CICIDS 2017 dataset for identification of attacked nodes. This scheme has achieved 73.79% accuracy but failed to reduce training and testing error [16]. In 2021, Arnold Adimabua Ojugo use deep neural network for attacked nodes identification. It works well in case of accuracy as well as elapsed time [17].In 2020, Bavani K use mathematical model for distributed DOS detection. This model has the capability to work well upto 500 data packets.Its accuracy rate is 97% [18]. In 2021, Sungwoong present LSTM based attack detection model. It has a 92% attack detection rate and 20% false positive rate [19]. In 2021, Deepak Kshirsagar introduced weight based reduction method for security attacks identification and prevention. It has a great accuracy which is upto 90% [20]. In 2020, Ademola P. Abidoye develop lightweight model for detection of DOS attack in wireless sensor network. Experimental result verify the accuracy and effectiveness of this system . They use network simulator NS3 for simulation of this scheme. It takes lot of time to train and test the model [21]. In 2021, Yasser Alharbi propose KNN algorithm for DOS attack detection. This algorithm improve attack detection performance of IPv6 network. This algorithm calculate distance between two sample points and finally get the attacked nodes. It has some deficiencies such as inaccuracy, false positive rate and it takes more time to identify attacked nodes [22]. In 2021, Dan Zhang present survey on attack detection and review about Deception attack and ICMP attacks. It includes advantage, disadvantage, conclusion and various methodologies [23]. In 2021, Amiya Kumar Sahu propose deep learning based mechanism to detect security attack in IOT devices. Its accuracy rate is 96% [24]. In 2021, Jun Zhang propose deep learning solution for cyber attack detection. They use several high quality dataset for simulation of such problem. They discuss challenges, shortcomings and future scope of such research [25]. In 2021, Bilal Alhayani investigate about different kinds of cyber security attacks like denial of service, phishing attacks etc. They plan strategies and apply in the network for security of data from different kinds of malware [26]. In 2022, Christopher Regan propose federated based approach to detect botnet attacks. Simulation result shows 98% accuracy rate and has a great performance over traditional methods [27]. In 2022, Sandeep Kautish propose DDOS strategy for cloud computing environment when we compare it with existing methods, it's accuracy is 96% [28]. In 2022, Qiuhua Wang focus deep learning based approach for cyber attack detection. Experimental result validate that it has 85% accuracy rate and are able to detect malicious modes within 200 seconds [29]. In 2022, Kim-Hung-Le present an intrusion detection software to protect vehicular communication from different kind of cyber attack such as wormhole, Backdoor etc [30].In 2022,vartika agarwal investigate about deep learning technique to improve RRM in VCN.They highlight various algorithm for resource allocation [31]. In 2022, Vartika Agarwal highlight multitype vehicle identification scheme from real time traffic database and offer subscription plan for its user[32].

TABLE I. Comparative Study

Author	Proposed Scheme	Advantage	Limitation or Future Scope
[1]	Security attack detection in SDN	70% accuracy, High precision	High packet drop rate as well as training and testing error
[2]	Survey of DDOS attack detection technique	Elaborate the Different kind of cyber security attacks	Results under this survey are less accurate.
[3]	Review on Cyber attacks	Details about effect of cyber attacks on a network	Future work on Cyber attacks on cloud , homes as well as IOT based systems.
[4]	Artificial Neural Network (ANN) for detecting cyber attacks	Offer satisfactory result in case of accuracy as well as detection time	Upgrade ANN for better accuracy.
[5]	Intrusion detection scheme with recurrent neural network	80% accuracy as well as less network drop rate.	Training time and testing time should be reduced.
[6]	Supervisory strategy for detecting attacker behaviour.	Packet reception rate is high.	Works only for limited no of nodes.
[7]	Supervised Machine learning algorithm for identifying normal nodes as well as an attacked nodes.	86% accuracy and achieve better performance.	Works only for NSL-KDD datasets.
[8]	Reviewed about different kind of cyber-attacks.	Covering 80 methods for analysing attacks.	In future, detection and prevention mechanism should be explored.
[9]	Attack detection through LSTM and RNN.	80% accuracy and less false positive rate.	Modify the proposed system for wormhole attack detection.
[10]	Attack detection in mobile adhoc network .	Different attack detection techniques are elaborated.	In future, explore some recent challenges in MANET.
[11]	Smart DOS attack detection system	Accuracy, high precision and low false alarm rate.	Modify this approach for better detection rate.
[12]	Gradient descent algorithm for cyber security attack.	Reduce training as well as testing error.	Use deep learning approach for more accurate result.
[13]	Machine learning algorithm for security attack detection.	Great result in term of accuracy as well as faster response time.	Combine several algorithm for better result.
[14]	Deep neural network for DOS attack detection	Less packet loss, less overhead as well as better throughput	Modify this approach for better result and implementing in real time environment.
[15]	Tensor based model for DDOS detection.	throughput rate is good as well as accurate result	Packet drop rate is too high.
[16]	DDOS attack detection on CICIDS 2017 datasets.	73% accuracy as well as less packet loss.	Reduce training and testing error.
[17]	Deep neural network for prevention of security attack.	70% accuracy and better throughput.	Use RNN or LSTM for better result.
[18]	DDOS detection in SDN	Highly accurate and work for 500 data packets.	Increase no of packets for better research.
[19]	LSTM based security attack detection.	92% attack detection rate and 20% false positive rate.	Reduce packet drop rate and increase the accuracy.
[20]	Weight based reduction method for security attack detection.	90% accuracy rate as well as less packet loss.	Apply this technique for different dataset.
	Proposed Scheme.	**99% attack detection accuracy as well as 2% reduction in training/testing error**.	**We can use this scheme to detect further attacks such as node replication, wormhole etc**.

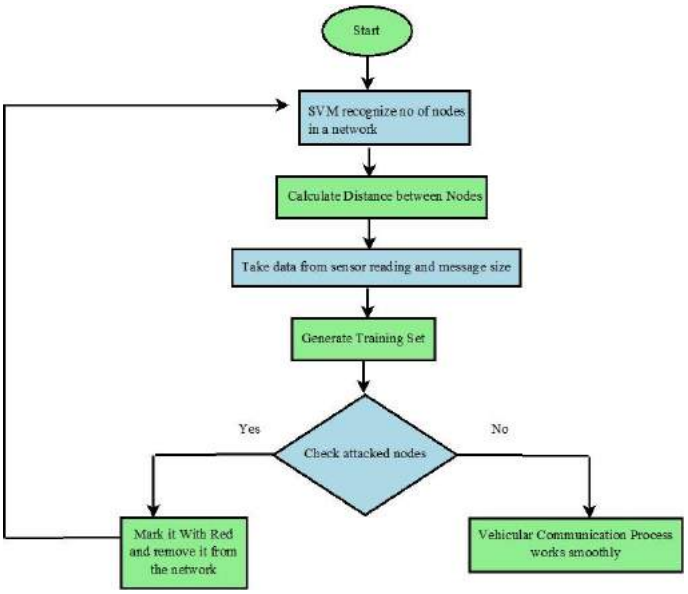

Figure 1. SVM for DOS detection

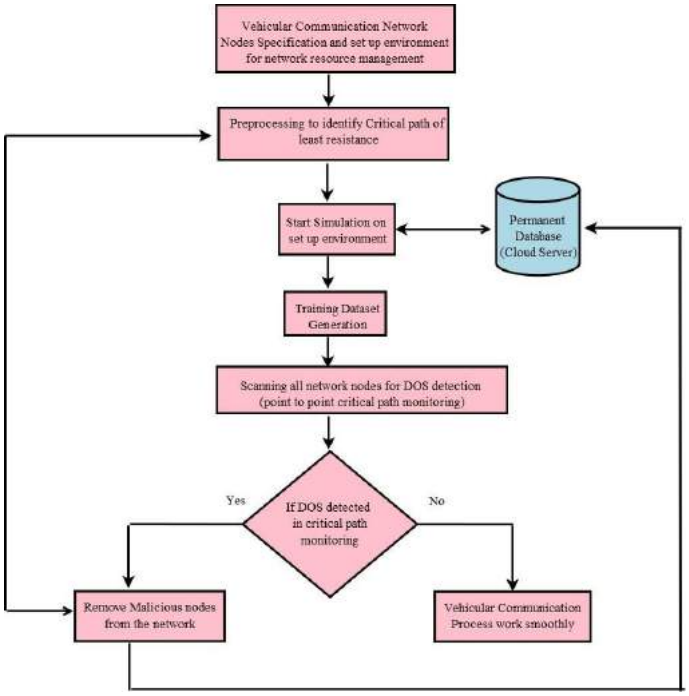

Figure 2. Flow chart of P2PCPM based DOS attack detection for vehicular communication network resource management

3. Methodology and Implementation

Our research focuses on DOS detection in a vehicular communication network using a support vector machine (SVM).The main objective of this research is to eliminate those nodes which disrupt the vehicular communication network.

i. **Vehicular Communication Network Resource Management**: It contains thousands of sensors of nodes. The node is equipped with various sensing devices and have a limited processing speed and storage capacity. In this simulation, we have to use sensor data that are taken from vehicles. Message Size which was transmitted by the attackers.

ii. **Support Vector Machine**: It is an algorithm that learns by example to assign tag to nodes. In proposed research SVM identify DOS attack by sensor reading and message size. After taking data, it recognizes those nodes which is responsible for communication interruption. It remove those nodes and offer safer communication.

From Figure 1, we can see that SVM recognize no of nodes (Vehicles) in VCN then SVM calculate distance from one nodes to another nodes. After it SVM takes data from sensor reading and message size and generate training set. After generating training set. SVM check nodes and classify it into two categories. If they are attacked nodes mark it with red, remove it from VCN . If there are no attacked nodes, vehicular communication process works smoothly. This process continue until all attacked nodes are not detected.

iii. **System Configuration**: Intel i5 processor with 8 GB RAM support this experiment. MATLAB 2020 have best features which are used for simulation for this research.

The steps for research design are shown in Figure 2. In this figure, we can see the whole process from vehicular communication network generation to attack detection. In every round, we can see that attacked nodes are detected and speed up the communication process between automobiles.

A. **Network Specification**: It includes all the inputs and output generated by user or system. User have to enter length and width of an area, reading of sensor, size of message etc. After entering input , system provide no of attacked nodes, no of rounds etc. (Table II) (Figure3)

TABLE II. SIMULATION PARAMETERS CONSIDERED IN IMPLEMENTATION

Parameters for Simulation	Value
Number of Nodes	100
Area Length	500
Area Width	500
Sensor Data	25
Message Size	500 bytes
Dimensions	1000*1000
Percentage of Attacked Nodes	up to 2%
Maximum no of rounds	50

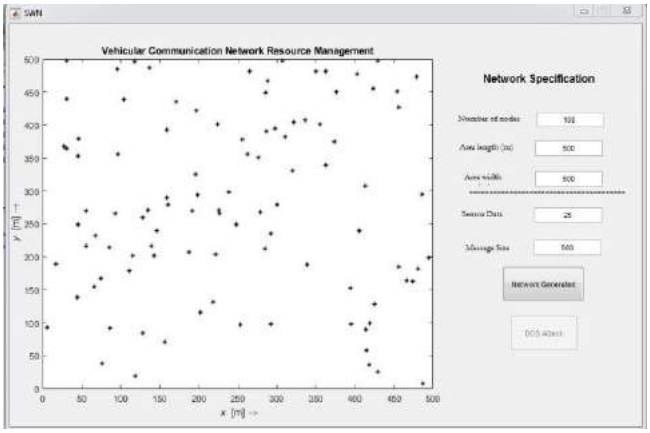

Figure 3. Simulation and Set up of Vehicular communication network resource management

B. **Network Nodes Specification**: After network specification, nodes according to the specification is generated. After the generation of nodes, the path of VCN is generated. (Table III) (Figure 4).

After generating critical path of vehicular communication network. We can get specification Evaluation matrix of point to point critical path network (Table IV).

TABLE III. POINT TO POINT CRITICAL PATH OF NETWORK NODES SPECIFICATION

S.No	**Starting Point**		**mid point**	**End Point**		**Radius**
	Longitude	**Latitude**		**Longitude**	**Latitude**	
X0	29.9457^oN	78.1462^oE	30.1311	30.3165^oN	78.0322^oE	0.1854
X1	29.9458^oN	78.1462^oE	30.1311	30.3165^oN	78.0322^oE	0.1853
X2	29.9459^oN	78.1462^oE	30.1312	30.3165^oN	78.0322^oE	0.1853
X3	29.9460^oN	78.1462^oE	30.1312	30.3165^oN	78.0322^oE	0.1852
X4	29.9461^oN	78.1462^o E	30.1312	30.3165^oN	78.0322^oE	0.1852
X5	29.9462^oN	78.1462^o E	30.1313	30.3165^oN	78.0322^oE	0.1851
X6	29.9461^oN	78.1462^oE	30.1314	30.3165^oN	78.0322^o E	0.1851
X7	29.9464^oN	78.1462^oE	30.1314	30.3165^oN	78.0322^o E	0.1877
X8	29.9465^oN	78.1462^oE	30.1315	30.3165^oN	78.0322^o E	0.185
X9	29.9466^oN	78.1462^oE	30.1315	30.3165^oN	78.0322^o E	0.184

C. **Generate Training Set**: After VCN generation, training set will be created and this model is verified on data very similar to real sensing data to check the power of this model to eliminate attacked nodes and calculate training as well as testing error.

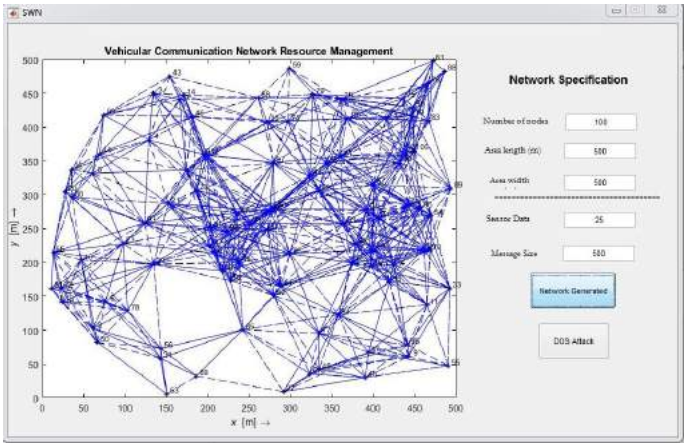

Figure 4. Vehicular communication network generation

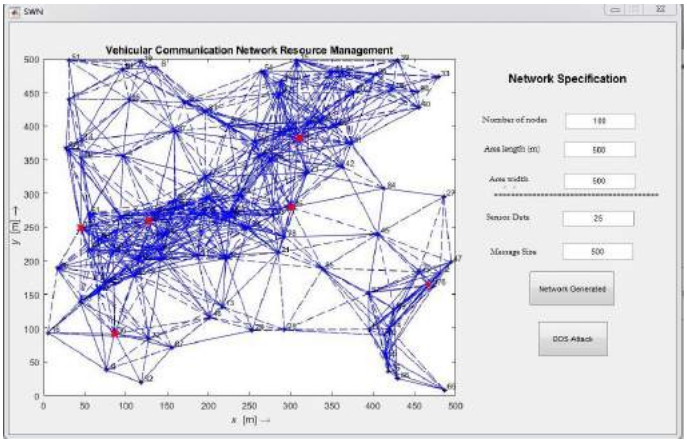

Figure 5. DOS attack detection in vehicular communication network resource management

TABLE IV. Specification evaluation matrix of P2PCPM (N=10)

Statistics	Result
Squared Deviation	8.9402
Variance	9.8
Covariance	33.479
Standard Deviation	500
Coefficient of correlation	10.69

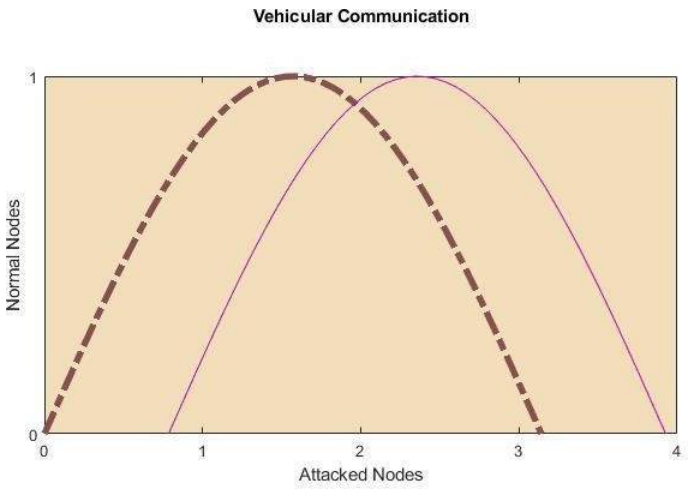

Figure 6. Normal nodes vs attacked nodes in vehicular communication network resource management

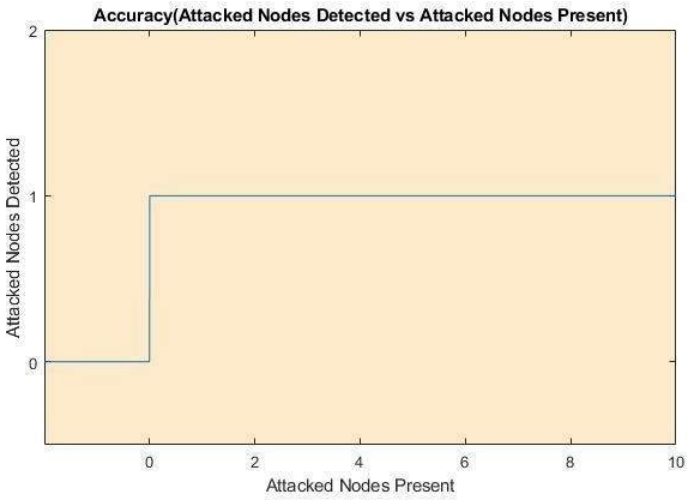

Figure 7. Proposed Methodology (P2PCPM)

D. **DOS Detection**: After Generating Datasets, we identified those vehicles which suffer from DOS attack. Red nodes will be marked as attacked nodes (Figure 5). From Table V, we can see that there are 6 bad nodes whose sensor data is above 25 and message size is 500. This process continues until bad nodes are detected

After the elimination of attacked nodes, speed of communication between vehicles will be increasing. From Figure 6, we see that dotted line represent attacked nodes and after identification of attacked nodes communication between vehicles increasing continuously.Here two different scenarios are the normal node and attacked node. In a Normal node, communication between nodes will continue otherwise in DOS attacked node, the message passing through that nodes automatically stops during the simulation of n no of nodes.

TABLE V. Training set generation in VCN resource management

Sensor Read	Message Size	Status	Sensor Read	Message Size	Status
14.638	206.7	-1	12.584	181.81	-1
9.3068	122.7	-1	11.049	168.65	-1
12.667	221.66	-1	11.503	222.01	-1
4.7519	205.15	-1	8.315	124.87	-1
11.596	171.48	-1	7.2621	189.59	-1
10.929	224.65	-1	9.331	124.74	-1
9.0646	164.62	-1	10.466	290.49	-1
11.738	132.6	-1	12.377	194.15	-1
12.194	112.28	-1	8.0237	261.31	-1
8.7763	224.75	-1	17.436	245.43	-1
8.4435	142.29	-1	14.801	262.88	-1
12.403	272.63	-1	11.184	207.83	-1
8.6055	96.159	-1	13.414	157.49	-1
9.7336	191.18	-1	5.9055	213.95	-1
9.4621	167.4	-1	15.059	229.85	-1
11.944	212.24	-1	25.374	501.44	1
8.6277	194.08	-1	25.37	486.98	1
9.685	135.53	-1	26.501	468.02	1
26.363	498.59	1	24.552	494.76	1
24.838	504.8	1	25.917	524.81	1
25.15	514.41	1	26.42	532.64	1
24.142	481.77	1	25.59	478.39	1
25.36	497.63	1	26.74	534.58	1
23.318	532.59	1	25.001	496.85	1
25.067	485.08	1	22.073	461.98	-1
26.56	516.8	1	28.512	500.57	-1
24.71	470.56	1	25.359	491.64	1
25.359	491.64	1	24.419	454.26	1
25.48	510.75	1	27.023	466.01	1
24.525	495.65	1	23.941	524.26	1
24.873	540.78	1	24.28	503.59	1
24.905	502.07	1	24.834	517.92	1
26.799	529.84	1	27.539	473.22	-1
23.777	532.97	1	8.3974	139.5	-1
10.927	202.6	-1	12.741	243.88	-1
9.0046	250.71	-1	9.7863	195.78	-1
15.933	107.32	-1	8.8152	145.16	-1
12.366	210.93	-1	12.045	239.71	-1
13.972	223.16	-1	11.315	169.37	-1
3.837	312.22	-1	7.8687	203.62	-1
11.279	243.28	-1	10.644	179.22	-1
14.906	144.25	-1	13.516	234.26	-1
11.242	251.88	-1	10.207	291.11	-1

4. Performance Evaluation and Discussion

For performance evaluation, we use following parameters accuracy, throughput and elapsed time. These parameters are basically used for validating the performance of the system.

Accuracy = (Attacked Nodes Detected*100)/(Attacked Nodes Present) 99% (Figure 7)

False Positive Rate (FPR) - It is the ratio of DOS Attacked nodes and those nodes which are classified as normal by mistake but belong to DOS attack.

FPR = (Number of misclassified DOS attacked nodes*100)/(Actually Attacked Nodes) = 1%

Elapsed Time - It means the time taken by the software to detect attacked nodes = 128 Seconds.

From Table VI, [12] author used gradient descent algorithm for identifying DOS attack. It has limitation that it works only for 41 nodes. Its takes 332 sec to train and 328 sec to test the model. [16] author used CICIDS 2017 dataset for DDOS detection but has less accuracy and takes lot of training as well as testing time. [17] author classify data packets into malicious and non malicious data packets. Its accuracy rate is 70% which is very less. [18] author detect DDoS attack in software defined network. It has 97% accuracy but it has limitation that it can identify malicious node upto 500 data packets. [19] author detect DOS attack using LSTM technique. It has 92% accuracy and 20% false positive rate. It takes 160 sec to train the model and 158 sec to test the model which is more in comparison of proposed scheme. [20] author propose intrusion detection system and reduce DDOS attack with 90% accuracy. limitation of this scheme is that it works only for CICIDS 2017 datasets.From above references, we can validate that proposed scheme works for more than 1000 nodes and provide 99% accurate result. Its false positive rate is 16% and reduces training as well as testing error upto 2%.

5. Conclusion and Future Scope

Major research gap we found that any scheme would not work for more than 500 nodes and there is a lack of accuracy. In the proposed approach, we can check DOS attack up to 1000 vehicle nodes. In this research, we are checking DOS attack upto 100 nodes out of which 6 nodes are attacked nodes. we can check attacked nodes again and again after changing network specification. Success rate is 99% in detecting DOS attacks. It takes 132 seconds for model training and 128 seconds for model testing. After detecting attacked nodes, communication process work smoothly(Figure.7). This scheme works well in comparison of other security detection models (Table VI). Experimental results demonstrate that this methodology offer more accurate outcomes. In future, we can use this scheme to detect further attacks such as wormhole,Node replication attack etc.

TABLE VI. Performance comparison of P2PCPM Based DOS detection with existing methodologies

Nodes Datasets	Accuracy	Training time	Testing Time	Reference
41	97.7%	332 Sec	328 Sec	[12]
CICIDS 2017	70%	288 Sec	285 Sec	[16]
CICIDS 2017	70%	175 Sec	173 Sec	[17]
500 Data Packets	97%	150 Sec	147 Sec	[18]
2018 Korea	92%	160 Sec	158 Sec	[19]
CICIDS 2017	90%	170 Sec	168 Sec	[20]
1000	**99%**	**132 Sec**	**128 Sec**	**Proposed Scheme**

References

1) Kim, M., Jang, I., Choo, S., Koo, J., Pack, S. (2017, September). Collaborative security attack detection in software-defined vehicular networks. In 2017 19th Asia-Pacific network operations and management symposium (APNOMS) (pp. 19-24). IEEE.

2) Bawany, N.Z., Shamsi, J.A. Salah, K. DDoS Attack Detection and Mitigation Using SDN: Methods, Practices, and Solutions. Arab J Sci Eng 42, 425–441 (2017).

3) Mahjabin, T., Xiao, Y., Sun, G., Jiang, W. (2017). A survey of distributed denial-of-service attack, prevention, and mitigation techniques. International Journal of Distributed Sensor Networks, 13(12), 1550147717741463.

4) Idhammad, M., Afdel, K., Belouch, M. (2017). Dos detection method based on artificial neural networks. International Journal of Advanced Computer Science and Applications, 8(4), 465-471.

5) Yin, C., Zhu, Y., Fei, J., He, X. (2017). A deep learning approach for intrusion detection using recurrent neural networks. Ieee Access, 5, 2195421961.

6) Su, L., Ye, D. (2018). A cooperative detection and compensation mechanism against denial-ofservice attack for cyber-physical systems. Information Sciences, 444, 122-134.

7) Rathore, S., Park, J. H. (2018). Semi-supervised learning based distributed attack detection

framework for IoT. Applied Soft Computing, 72, 79-89.

8) Navarro, J., Deruyver, A., Parrend, P. (2018). A systematic survey on multi-step attack detection. Computers Security, 76, 214-249.

9) Fu, Y., Lou, F., Meng, F., Tian, Z., Zhang, H., Jiang, F. (2018, June). An intelligent network attack detection method based on rnn. In 2018 IEEE Third International Conference on Data Science in Cyberspace (DSC) (pp. 483-489). IEEE.

10) Liu, G., Yan, Z., Pedrycz, W. (2018). Data collection for attack detection and security measurement in mobile ad hoc networks: A survey. Journal of Network and Computer Applications, 105, 105-122.

11) Lima Filho, F. S. D., Silveira, F. A., de Medeiros Brito Junior, A., Vargas-Solar, G., Silveira, L. F. (2019). Smart detection: an online approach for DoS/DDoS attack detection using machine learning. Security and Communication Networks, 2019.

12) Rajakumaran, G., Venkataraman, N., Mukkamala, R. R. (2020). Denial of Service Attack Prediction Using Gradient Descent Algorithm. SN Computer Science, 1(1), 1-8.

13) Susilo, B., Sari, R. F. (2020). Intrusion Detection in IoT Networks Using Deep Learning Algorithm. Information, 11(5), 279.

14) Sumathi, S., Karthikeyan, N. (2020). Detection of distributed denial of service using deep learning neural network. Journal of Ambient Intelligence and Humanized Computing, 1-11

15) Maranhão, J. P. A., da Costa, J. P. C., Javidi, E., de Andrade,C. A. B., de Sousa Jr, R. T. (2021). Tensor-based framework for Distributed Denial of Service attack detection. Journal of Network and Computer Applications, 174, 102894.

16) Sambangi, S., Gondi, L. (2020). A Machine Learning Approach for DDoS (Distributed Denial of Service) Attack Detection Using Multiple Linear Regression. In Multidisciplinary Digital Publishing Institute Proceedings (Vol. 63, No. 1, p. 51).

17) Ojugo, A. A., Yoro, R. E. (2021). Forging a deep learning neural network intrusion detection framework to curb the distributed denial of service attack. International Journal of Electrical and Computer Engineering, 11(2), 1498.

18) Bavani, K., Ramkumar, M. P., GSR, E. S. (2020, March). Statistical Approach Based Detection of Distributed Denial of Service Attack in a Software Defined Network. In 2020 6th International Conference on Advanced Computing and Communication Systems (ICACCS) (pp. 380-385). IEEE.

19) Yeom, S., Choi, C., Kim, K. (2021, March). Source-side DoS attack detection with LSTM and seasonality embedding. In Proceedings of the 36th Annual ACM Symposium on Applied Computing (pp. 1130-1137).

20) Kshirsagar, D., Kumar, S. (2021). An efficient feature reduction method for the detection of DoS attack. ICT Express.

21) Abidoye, A. P., Kabaso, B. (2021). Lightweight models for detection of denial-of-service attack in wireless sensor networks. IET Networks, 10(4), 185-199.

22) Alharbi, Y., Alferaidi, A., Yadav, K., Dhiman, G., Kautish, S. (2021). Denial-of-Service Attack Detection over IPv6 Network Based on KNN Algorithm. Wireless Communications and Mobile Computing, 2021.

23) Zhang, D., Wang, Q. G., Feng, G., Shi, Y., Vasilakos, A. V. (2021). A survey on attack detection, estimation and control of industrial cyber–physical systems. ISA transactions, 116, 1-16.

24) Sahu, A. K., Sharma, S., Tanveer, M., Raja, R. (2021). Internet of Things attack detection using hybrid Deep Learning Model. Computer Communications, 176, 146-154.

25) Zhang, J., Pan, L., Han, Q. L., Chen, C., Wen, S., Xiang, Y. (2021). Deep learning based attack detection for cyber-physical system cybersecurity: A survey. IEEE/CAA Journal of Automatica Sinica, 9(3), 377-391.

26) Alhayani, B., Abbas, S. T., Khutar, D. Z., Mohammed, H. J. (2021). Best ways computation intelligent of face cyber attacks. Materials Today: Proceedings.

27) Regan, C., Nasajpour, M., Parizi, R. M., Pouriyeh, S., Dehghantanha, A., Choo, K. K. R. (2022). Federated IoT security attack detection using decentralized edge data. Machine Learning with Applications, 100263.

28) Kautish, S., Reyana, A., Vidyarthi, A. (2022). SDMTA: Attack Detection and Mitigation Mechanism for DDoS Vulnerabilities in Hybrid Cloud Environment. IEEE Transactions on Industrial Informatics.

29) Wang, Q., Yang, H., Wu, G., Choo, K. K. R., Zhang, Z., Miao, G., Ren, Y. (2022). Black-box adversarial attacks on XSS attack detection model. Computers Security, 113, 102554.

30) Le, K. H., Nguyen, M. H., Tran, T. D., Tran, N. D. (2022). IMIDS: An Intelligent Intrusion Detection System against Cyber Threats in IoT. Electronics, 11(4), 524.

31) Agarwal, V., Sharma, S. (2022). Deep Learning Techniques to Improve Radio Resource Management in Vehicular Communication Network. In Sustainable Advanced Computing (pp. 161-171). Springer, Singapore.

32) Agarwal, V., Sharma, S. (2022). EMVD: Efficient Multitype Vehicle Detection Algorithm Using Deep Learning Approach in Vehicular Communication Network for Radio Resource Management .

"**Vartika Agarwal** received degree of Bachelor of Computer Application from Surajmal Agarwal Pvt Kanya Mahavidyalaya, Kichha, and Uttarakhand, India. She obtained master of computer application degree from Shri Ram Murti Smarak College of Engineering and Technology (SRMS), Bareilly, Uttar Pradesh India. She is currently pursuing Ph.D. in Computer Science and Engineering Department from Graphic Era Deemed to be University, Dehradun, Uttarakhand, India. Her research interests include Internet of Things, Image Processing, Computer Vision etc."

"**Sachin Sharma**, Associate Professor , Department of CSE at Graphic Era (Deemed to be) University, Dehradun, Uttrakhand, India. He is Co-founder of IntelliNexus LLC. He has completed his Ph.D. from University of Arkansas at little rock in the subject of engineering science and system specialization. He has a great knowledge about wireless communication networks, IOT, Vehicular adhoc networking and network security"