Proposed Hybrid Secured Method to Protect Against DDOS in n Vehicular Adhoc Network (VANET)

https://doi.org/10.3991/ijim.v17i11.38907

Tuka Kareem Jebur
Department of Accounting, Al-Mustansiriyah University, Baghdad, Iraq
tukakareem@uomustansiriyah.edu.iq

Abstract—Security and safety are critical concerns in Vehicular Adhoc Network. vulnerable to Distributed Denial of Service (DDoS) attacks, which occur when multiple vehicles carry out various tasks. This cause disrupts the normal functioning of legitimate routes. In this work, the Hybrid PSO-BAT Optimization Algorithm (HBPSO) Algorithm based on modified chaos -cellular neural network (Chaos - CNN) approaches has been proposed to overcome DDoS attacks. The suggest approaches consists of three-part which are hybrid optimization search algorithm to enhance the route from source to destination, chaos theory module is used to detect the abnormal nodes, then on Modified Chaotic CNN (MCCN) employed to prevent a malicious node from sending data to the destination by determining node that consumer more resource, packets lose or the victim could reset the path between the attacker and itself. CICIDS dataset has been used to test and evaluate the performance of the proposed approach based on the criteria of accuracy, packet loss, and jitter. The Chaos - CNN approached results to outperform similar models of the related work and the approach protects the VANETs with high accuracy of 0.8736, specificity of 0.9959, TPR of 0.9561, and FPR of 0.78, Detection rate 0.9561.

Keywords—Vehicular Adhoc Networks (VANETs), Intrusion Detection System (IDS), Distributed Denial of Service (DDoS) attack, chaos -cellular neural network (Chaos - CNN), particle swarm optimization, Bat optimization

1 Introduction

As a result of the development in smart devices and software, the emergence of many advanced software and companies competing to produce models Sophisticated software and the increasing demand for smart systems, which is due to the rapid increase of vehicles on the road every day due to traffic jams for long periods [1]. VANETs considered a subset of Adhoc Systems, Moving cars in cities and highways, and converting each car into a network participant, into a wireless router that allows cars to move away from each other at a distance of approximately 300 meters .The attacks that this network suffers from where users cannot analyze the resources in the event of an attack DDOS [2]. Because of the transmission of critical messages in VANETs, the availability re-

quirement should be prioritized among these requirements. If the availability of a message is jeopardized due to any issue, it can result in a life-threatening situation [3]. The groups that face this type of network are denial-of-service attacks due to the loss of security in this type of network, so there are many attempts to compensate for the deficiency in this aspect, where the problem of loss of security is the result of the network as a result of the network topology. A single source attack in Denial of Service (DOS) attacks, while DDoS uses multiple hosts to attack a network [4], [5]. The authorized users cannot determine resources in the case3of a DDoS attack.

Chaos offers a more accurate and efficient identification of network abnormal activity that reduces the false positive caused by the subjective factors of man [6]. Chaos - CNN enables the internal representation of the hidden layer to be read directly. MENN training algorithms are substantially quicker than multilayer phrases (MLPs) however (Chaos -CNN) used to defiance agents' malicious nodes in MANET. The attacks by DDoS pose significant challenges to VANETs network accessibility. In this work, the Hybrid PSO - Bat Optimization algorithm and the Algorithm based Chaos -CNN approaches have been proposed to overcome DDoS attack. Chaos -CNN approaches consist of three-part which are, Hybrid PSO - Bat Optimization algorithm clustering area to improve the route from origin to destination, chaos theory module is employed to detect the abnormal nodes, then Chaos –CNN employed to prevent a malicious node from sending data to the destination by determining node that consumer more resource, packets lose or the victim could reset the path between the attacker and itself. The remainder of this work is as follows: Section 2 includes a review of related literature. Section 3 describes the methodology ad Section 4 discusses the results of the experiment. Section 5 brings the work to a close.

2 Related works

This research paper was presented in order to analyse and study DDOS in a network quickly and accurately in the event that this type of network shows abnormal behaviour, as many programs and algorithms were used, including packets, Bloom filters and other techniques among the traditional techniques, where security is among the most important goals that this type of network loses.[7], [8]. As a result, we are more explicit and focused on this subject, as shown below. In [9], the ideal ant technique was used for the purposes of collecting information, verifying the network environment, where this algorithm contributed to identifying the sent packets, determining what kind of data was lost during transmission, and abnormal behavior in the case of determining the type of attacks on this type of network, which are DDOS attack , which are studied here. The nearby nodes in the network and collecting information were updated with this algorithm using the Moore-based cellular automata and this type of update was used to determine which nodes in the network the attack is taking place. In [10], the researcher used the ant colony algorithm with chaos theory in order to detect DDOS, where the best nodes eligible for transmission in the network were determined by determining the abnormal behaviour of the nodes within the network and redirecting the data to the best path from the source to the recipient Thus, the attacks are determined based on the

abnormal behaviour of any node within the network, so that the severity of the attack was carefully studied and a procedure to take the correct action during the traffic routing process. additionally in [11], the researcher here is using an ant algorithm to reduce the load on the network and determine the transmission of data from a source to the network interface or node, choosing the best transmission path, the rest of the data is missing by identifying denial-of-service attacks. In [12], the swarm algorithm was proposed, the ant algorithm, PSO-ACO where this proposed hybrid algorithm was used to solve the problem of network mobility and data loss by solving the problem of load balancing in networks.

3 System model

This study developed an algorithm that employs the trust model and the cuckoo search algorithm. To mitigate the effects of a DDoS attack, the second phase employs chaos theory to control network traffic and detect abnormalities in malicious nodes, while the third phase employs fuzzy logic to compare with the suggested method. We discussed the research methods and materials of this work in this section, beginning with a review of the hybrid PSO-BAT (HPSO-BAT), Chaos Theory-CNN Neural Network (Chaos-CNN) architecture, and mechanisms related to this work. Following that, the CIDDS testing dataset and its attributes were described. Following that, we explain the threats model design and the evaluation methods used.

3.1 Testing dataset

Performance tests for intrusion detection systems (IDS) and intrusion prevention systems (IPS) are performed using a variety of datasets such as the KDD, DEFCON, and others. The CICIDS 2017 dataset [13] was chosen from among these various types of datasets based on the various features that can be used to evaluate the performance of our model. In this analysis, the available CICIDS 2017 data set was used to test the performance of the proposed model. Table 1 depicts the CICIDS features.

Table 1. The CICIDS features [13]

Feature name	Weight
Fwd. IAT. Total	46.083171
Flow. IAT. Max	39.047967
Active. Max	38.372911
Active. Min	37.004728
Fwd. IAT. Max	36.595626
Active. Mean	35.621885
Idle. Min	33.588032
Idle. Max	32.288567
Flow. IAT. Std	29.902196
Fwd. IAT. Mean	28.631780

3.2 Particle swarm optimization (PSO)

Using social psychology, it Searching for the optimal solution in the specified area, and in general, the greater the number of elements of the swarm and the smallness of the search area, the faster and easier the optimal solution can be found in the least possible time and vice versa, that is, the greater the number of elements removed from the used area and the small number of elements, the more difficult it will be to find the optimal solution [14].

3.3 The Bat algorithm

It is one of the algorithms inspired by living creatures, the bat algorithm and is inspired by the behavior of bats in echolocation at rates varying in oscillation emission and loudness, Where the algorithm can be represented as follows [15]:

1. Echolocation is used by all bats to identify prey and obstacles based on sound frequencies received.
2. All bats fly at random with velocity (vl) at position (yl), and the values for frequency, loudness, and wavelength are fl, A0, and respectively.
3. The loudness shifts from a high positive (A0) to a low positive value (Amin).
   Bat sounds have a pulsation rate (rl) that ranges between 0 and 1. The number one means that the pulsation rate has reached its maximum, and 0 means that it has reached its minimum. The following equations [3] are used to update the velocity, frequency, and position:

$$fl = fmin + (fmax - fmin) \times \beta \tag{1}$$

$$vl\ (t) = [yl\ (t - 1) - Y*] \times fl \tag{2}$$

$$yl\ (t) = yl\ (t - 1) + vl\ (t) \times t \tag{3}$$

where fl is the frequency, fmin is the minimum frequency, fmax is the maximum frequency, Y is the best position for the bats, t is the time step, yl (t 1) is the bats' position at time t 1, vl (t) is the velocity, and is the random vector.

3.4 Chaos theory (CS)

Chaos theory is can be considered a branch of mathematics, where this science focuses on studying the states of dynamic systems. Are these systems governed by several laws, including its starting point [16]. Chaos theory is a multidisciplinary theory. Where a slight change in the system in one case can lead to a big difference in later cases, i.e. the dependence of the starting point or the initial conditions are considered sensitive to generate the final conditions where a butterfly can flapping its wings in China can cause a hurricane in other cities such as Texas [17].

3.5 Cellular Neural Network (CNN)

There are many systems that need to process microprocessors and operations, and among these systems is the image processing system, and as a result, image processing does not depend on the processing pattern in real time and sequentially CNN its types of neural networks are used in the processing and the organization of this type of network is C networks It is considered one of the dynamic networks, non-linear and continuous, and it is one of the networks used in parallel computing [18].

3.6 Bloom filter

This filter can be tested from the filters that are used in operations that need high efficiency Use of space How this filter is used extensively to select and determine if this element that is assigned belongs to a group or not where there are several possibilities for a false positive match but there is no probability When this filter is used in the presence of false negatives, the bloom filter is working for permanent blocks of the attack IP address [19].

3.7 The hybrid PSO - bat optimization algorithm and Modified Chaotic CNN (MCCN)

Many methods have been proposed to defend against DDoS attacks as discussed in the literature but the performance is still not good enough. This work proposes thepso-bat Search Algorithm-based **Modified Chaotic CNN (MCCN)** to protect routing functions in MANETs against DDoS attack traffics. The hybrid PSO –BAT - MCNN monitors and controls DDoS traffics. This method monitors and analyze the incoming traffics by using Chaos Theory, any node with suspension behavior such as huge power consumer and movement and the relationship between source IPs and destination IPs will be detected as a malicious node. Figure 1 shows the architecture of the HPSOBAT - MCCN model. The model consists of three modules, which are Algorithm (HPSO-BAT), **Modified Chaotic CNN (MCCN),** and Chaos Theory (CS) as described below:

This section defines the work being proposed to improve IDS to detect and mitigation of DDoS.

1. First step Input network parameter upload data set that called (CICIDS) to Cuckoo search optimization algorithm, this algorithm gathers input data as clustering for route discoveries and better route selection according to coverage and CH then find the route and optimal CH in cluster determine out layer CH and saving IP address of nodes in a buffer.
2. The second step used chaos theory to detect abnormal nodes by controller network traffic with some parameters such: Average time, Specificity, False Positive Rate, and True Positive Rate accuracy. if the discover node as DDoS then go back to the first step, so the network output parameter is calculated with chaos theory and then the attacker is identified by MCCN if not determine the abnormal traffic the node

will be sent to bloom filter As previously stated, predefined parameters and traffic equate to permanent blocks for Demon IP address.

3. Third step applying MCCN to mitigation of DDoS in the VANET network. Based on the attacker's activities, the kind of attacker is being checked and the attacker The achievement of the best results is determined.

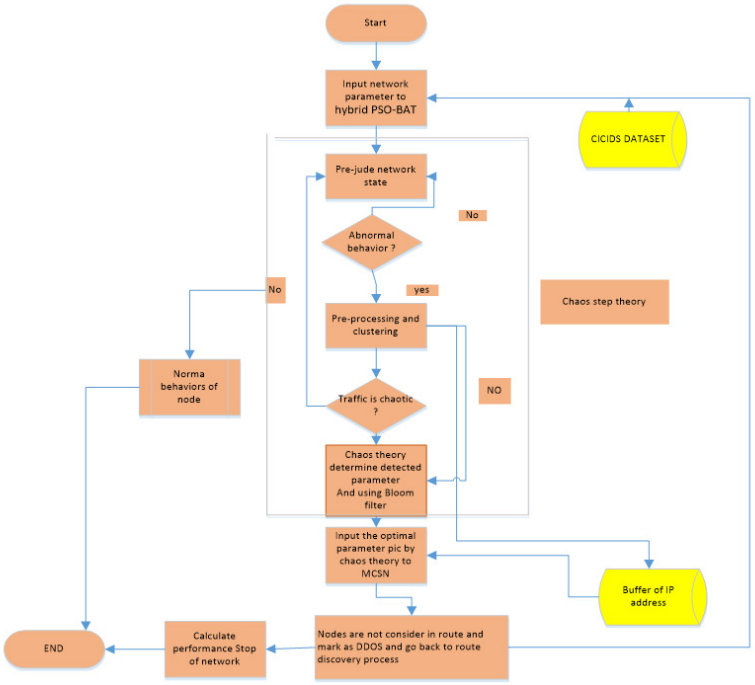

Fig. 1. The Proposed Method

3.8 Modified Chaotic CNN (MCCN) for optimal path finding and prevent a malicious node

This algorithm was proposed to find the best path between two nodes in the network without consuming a large amount of energy or taking a large time [20-25] In order to make the CNN network more efficient and effective, it has been proposed or used Ressler chaos system in the learning process of the network in order to increase the speed of learning and achieve the best acceptable results.

Pseudocode Hybrid pso-bat optimization algorithm

```
1. Input: Input dataset for training
2. Input file dataset for testing
3. Output: picked optimal CH and construction the value
4. Step1: generate the randomness placed of the VANET.
  (a)  For every i in Total_Vehicles
```

(b) Vx(i)=1000*runif(1) / Vx and Vy are the x and y coordinates of a vehicle
(c) Vy(i)=1000* runif(1)
(d) Fix(V(i), Vy(i))
(e) End For

5. Step2: To decide the coverage set of VANET
   (a) 1. For each i in 1:5 The number of iteration is 5
   (b) 2. For each j in 1: Total _Vehicles
   (c) 3. dist<-sqrt((rx[i]-vx[j])^2-(ry[i]-vx[j]^2))
   (d) 4. if (dist < 200)
   (e) cov_set[i,j]<-1
   (f) else
   (g) cov_set[i,j]<-0
   (h) End If
   (i) End For
   (j) End For
6. Step3: Define objective function f(x),x=(x1, x2, x3,--------)
7. Do initialization of a population of n bats /PSO swarm in erratic locations. parameter initializations and PSO examine parameter initializations
8. for it=1:N
9. New_Swarm =Get_PSO (Swarm ,Bestswarm ,Lowerbound,Upper-bound);
10. [fnew,Best,Swarm ,Fitness]=Get_Best_Swarm (Swarm ,New_Swarm ,fitness);
11. N_iteration =N_iterations+n;
12. New_Swarm =Empty_Swarm s(Swarm ,Lowerbound,Upper-bound,pa); [fnew,best,swarm ,fitness]=get_Best_Swarm (swarm ,New_Swarm ,fitness); N_iter=N_iter+n;
13. if fnew<fmin,
14. fmin=fnew; Bestnet=Best; // predict attack node
15. end
16. end
17. get the local best solution(Lbest)using PSO Q(i)=Qmin+(Qmax-Qmin)*rand // pick optimal CH (to de-crease time to send and received packet)
18. v(i,:)=v(i,:)+(swarm (i,:)*CBEST*Q(i); s(i,:)=swarm (i,:)+v(i,:);
19. if rand> r(it+1)
20. s(i,:)=cbest+0.0001*rand(1,D); end
21. Fnew=fobj(s(i,:));
22. if(Fnew<=fitness(i))&(rand<A(it+1))
23. swarm (i,:)=s(i,:);

```
24. fitness(i)=Fnew;
25. end
26. end
```

Algorithm 1: the proposed MCCNN for to mitigation of DDoS in the VANET network. prevent a malicious node

Input: patterns paths of nodes, m: clusters number, number of intra path p1, inter path p2, number of CH, α, ν, Rc(Ressler chaos), Lc(Lorenz chaos)

Output: find the optimal path and checked the attacker The achievement of the best results is determined.

- **Step1:** Generate Matrices $S, \hat{S}$.
- **Step2:** Initially, the MCCNN (with cells M1,N = Number of rows and columns of the 2D CNN equal to the number of wireless network nodes) obtains the input parameters, initial conditions, and learned templates. Load the wireless network clusters' all paths information. In addition, load the best other wireless node parameters (clusters size regions, packed size, Dynamic or non-dynamic, link costs, and bitrate).
- **Step3**. Set the weight vector to zero. Weight is kept constant while the hidden to output weights are learned with the shortest possible distance.
- **Step4:** converge cells
- while (converged-cells < total number of cells)
- {for (i1=l; i1<=M1; i1++)
- for (j1=l; j1<=N; j1++)
- {if (convergences[i1] [j1]) continues; // the current cells was converged //
- **Step5:** MCCNN reduction using algorithm 1.
- **Step6:** Activate the cells and get Q from all paths results as the short path whose is minimum E_{i1j1} as Q = min(E_{i1j1}) that optimized by other wireless nodes parameters (clusters size regions, packed size, (Dynamic or non-dynamic), link costs).
- **Step 7:** Calculate the next state using stored templates for the optimal path between p1 and p2.

$$x_{i1j1}(t+1) = x_{i1j1}(t) + \sum_{k,l \in N_{i1j1}} a_{k-i1,l-j1}\, f\left(x_{kl}\,(t)\right) + \sum_{k,l \in N_{i1j1}} b_{k-i1,l-j1}\,\left(u_{kl}\,(t)\right) - Lc + I$$

- where x_{ij}: the states of a cell at position(i1,j1),
- N_{ij}: the neighbors of the cell (i,j),
- a_{kl} : the parameters of feedback templates (Links connection weights),

- b_{kl} : the feedforward template parameters,
- u_{kl}: the (time-invariant) input,
- I: is a bias value.
- the smallest's Euclidean's distances of B_{ij} will select:
- B_{ij} = Q $\sum\sum_{j,i=1,2..m}$ ‖p1-p2‖
- and optimized by other wireless nodes parameters (clusters size regions, packed size, (Dynamic or non-dynamic), link costs).
- **Step8**: re-check the convergence criteria after the reduction operation.
- If $\left(\frac{dx_{i1j1}(t_n)}{dt}\right) = 0, and\ y_{lk} = \pm 1, \forall c(k,l) \in N_r(i1,j1)$
- {convergences[i1][j1] = 1;
- convergedcells++ ;} } /* end for loops */
- **Step9**: Update the entire paths state values.
- for (i1=l; i1<=M1; i1++) for (j1=l; j1<=N1; j1++)
- { if (convergences[i1][j1]) continue; $x_{ij}(t_n) = x_{ij}(t_{n+1})$; }
- iterations++;} /* end while */

End

4 Performance analysis

In this section, an analytical study is presented, comparing the results based on many measures. Evaluation used qualitatively and quantitatively. Several criteria have been applied to determine the detection of attacks using a set of data and their application to find privacy. What I know is how long it takes when sending data from the source to the target and how much data Which has been lost and among these criteria are matrix include true positive (TP), true negative (TN), false positive (FP), and false-negative (FN).

$$FPR = \frac{FP}{FP+TN} \tag{5}$$

$$TPR = \frac{TP}{TP+FP} \tag{6}$$

$$Accuracy = \frac{TN}{TN+FP} \tag{7}$$

Wherein, the accuracy stated as in Eq. 4.

$$Accuracy = \frac{TP+TN}{TP+FP+TN+FN} \tag{8}$$

The number of cases that are accurately categorized as normal is specified as TN in this passage. The number of occurrences that are correctly categorized as attacks is

represented by TP. The number of attack instances that were misclassified as normal occurrences is known as FP. Similar to FN, attack occurrences that were mistakenly classed as normal instances are counted. The ratio of all correctly classified cases (TP, TN) to all instances is how accuracy is measured (TP, TN, FP, and FN).

The absence of one or more information packets traveling through the computer network is known as packet losspacket, and it is calculated as Eq. 9.

$$Packet\ loss = \frac{number\ of\ packed\ lose}{number\ of\ packed\ sent} \tag{9}$$

5 Results and discussion

Here in this part of the research, the results obtained by applying the previously mentioned algorithms are described, what are the main reasons for using these techniques and what are the criteria that were used to select parameters in order to measure performance in terms of average transmission, amount of data loss or time consumed When sending from the source to the recipient and the amount of energy consumption that has been calculated, where the results are discussed and analysed in a large and accurate way in this part of the. The explanation for the same is given below:

- Average time ratio of time that calculates from source to destination node.
- Packet loss or drop occurs if the destination of one or even more data packets passing through the computer network fails. Packet loss is triggered by data transfer errors in wireless networks, generally. can be described as:

Figure 2 gives information about the comparison between PSO and HBPSO-MCCN based on the criteria of accuracy and Specificity. According to the obtained results, it is observed that the HBPSO-MCCN model of an accuracy of 0.9551 and specificity of 0.9959. Furthermore, When the malicious node is discovered, its contents are delivered to the other node, and therefore the transmission process is considered incorrect data, but it is largely in the network, which leads to the disconnection or sending fake responses about the delivery of data to the appropriate interface, so when applying this model, the detection is accurate and large for malicious or harmful nodes and they are placed in a case from the blacklist.

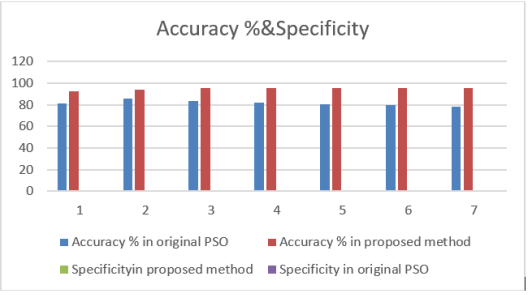

Fig. 2. Comparison between PSO and HBPSO-MCCN

Table 2 shows the comparison between the PSO and HBPSO-MCCN based on the criteria of accuracy and Specificity. Based on the obtained results it is observed that the HBPSO-MCCN achieved an excellent result with an accuracy.

Table 2. Accuracy and Specificity in deferent method

No. of Node	Accuracy		Specificity	
	PSO	***HBPSO-MCCN***	***PSO***	***HBPSO-MCCN***
10	0.8132	0.8736	0.8736	0.9959
20	0.8533	0.8736	0.8736	0.9959
30	0.8334	0.8736	0.8736	0.9959
50	0.8215	0.8736	0.8736	0.9959
100	0.8036	0.8736	0.8736	0.9959
150	0.7957	0.8736	0.8736	0.9959
200	0.7778	0.8736	0.8736	0.9959
Overall	**0.8140**	**0.8736**	**0.8736**	**0.9959**

Moreover, Table 3 shows the rate of detection of the system proposed is NOT the same as the PSO. It is because improvements in the approach to the database do not impact the consistency of attack detection. One of the benefits of the proposed approach is that the true positive rate and the false-negative rate remain virtually constant while reducing the time to detect an attack.

As illustrated in Table 3 the attack is more rapidly detected in the proposed method than in any other method due to filter bloom. The findings show that data from the reference database profile have to be retrieved through tuples. In any reference database, the time for reviewing, restoring, and executing is as high as three functions. On the other side, All the information required to detect an attack by using the data structure is provided in proposed and storage operations can be performed on time.

Table 3. Different periods in TPR and FPR

Time interval	TP	FP	Total Normal packets	Total attack packets	TPR (%)	FPR (%)
5	80860	7307	651686	73524	0.9561	1.26
10	80558	7005	651686	73524	0.9561	1.2
20	80256	6703	651686	73524	0.9561	1.14
30	79954	6401	651686	73524	0.9561	1.08
40	79652	6099	651686	73524	0.9561	1.02
60	79350	5797	651686	73524	0.9561	0.96
80	79048	5495	651686	73524	0.9561	0.9
90	78746	5193	651686	73524	0.9561	0.84
100	78444	4891	651686	73524	0.9561	0.78

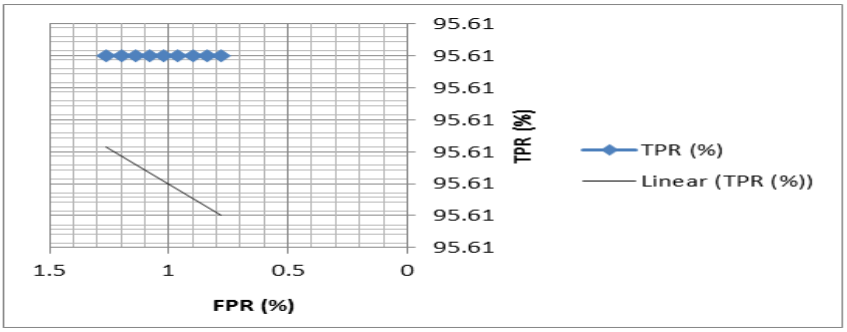

Fig. 3. The curve of FPR and FTR

However, no false positives and 100 percentage negatives have been detected. That's a reality. Perfect classification. The highest-ranking point in this figure is (0.72, 95.51), where the time interval of detection is around 60 seconds. Complete details and our knowledge in Table 4 Results of detection are provided.

Table 4. Comparison of the proposed method with existing techniques

Method	Accuracy	Detection rate	False alarm rate
Fuzzy logic [26]	0.6576	0.7859	5.79
Fuzzy Logic [27]	---	---	---
SVM [28]	0.9725	---	2.75
HBPSO-MCCN	0.9951	0.9561	~ 0

6 Conclusions

This article paper suggests the method to detect and prevent DDOS attack by using PSO-BAT algorithm as clustering method, chaos to monitoring traffic network of VANETs, modified chaos cellular Neural Networks (HBPSO-MCCN) to defines agents DDOS this method optimized to enhance the accuracy, a method for accelerating DDoS bandwidth attack detection in real-time is suggested in this paper. To decrease the information exchange with the database and thus the time of attack detection, and effective dataset known as CICIDS has been proposed. In this arrangement, data is stored at the lowest possible space to store the number of bits simultaneously in each byte. All data monitoring is stored in memory so that the database does not have to be referred to each monitoring time. This deletes update and refreshes operations, and storage is performed in the database at adjustable times. Reduce time prevent an attack and find the optimal path with reduced packet drop, average time will reduce.

Declaration of competing interest

"Have no any known financial or non-financial competing interests in any material discussed in this paper."

7 Reference

[1] W. Liang, Z. Li, H. Zhang, S. Wang, and R. Bie, "Vehicular Ad Hoc networks: Architectures, research issues, methodologies, challenges, and trends," *Int. J. Distrib. Sens. Networks*, vol. 2015, 2015. https://doi.org/10.1155/2015/745303

[2] B. A. Khalaf *et al.*, "A simulation study of syn flood attack in cloud computing environment," *AUS J.*, vol. 26, no. 1, pp. 188–197, 2019, doi: 10.4206/aus.2019.n26-1.19/.

[3] A. Saied, R. E. Overill, and T. Radzik, "Detection of known and unknown DDoS attacks using Artificial Neural Networks," *Neurocomputing*, vol. 172, no. August 2015, pp. 385–393, 2016. https://doi.org/10.1016/j.neucom.2015.04.101

[4] X. L. Hua, I. Gondal, and F. Yaqub, "Mobile agent based artificial immune system for machine condition monitoring," *Proc. 2013 IEEE 8th Conf. Ind. Electron. Appl. ICIEA 2013*, pp. 108–113, 2013. https://doi.org/10.1109/ICIEA.2013.6566349

[5] T. Zhou, R. R. Choudhury, P. Ning, and K. Chakrabarty, "P2DAP - Sybil attacks detection in vehicular ad hoc networks," *IEEE J. Sel. Areas Commun.*, vol. 29, no. 3, pp. 582–594, 2011. https://doi.org/10.1109/JSAC.2011.110308

[6] K. Adhikary and S. Bhushan, "Recent techniques used for preventing DOS attacks in VANETs," *Proceeding - IEEE Int. Conf. Comput. Commun. Autom. ICCCA 2017*, vol. 2017-Janua, pp. 564–569, 2017. https://doi.org/10.1109/CCAA.2017.8229864

[7] H. Hasrouny, A. E. Samhat, C. Bassil, and A. Laouiti, "VANet security challenges and solutions: A survey," *Veh. Commun.*, vol. 7, no. January, pp. 7–20, 2017. https://doi.org/10.1016/j.vehcom.2017.01.002

[8] W. Gao and S. Liu, "Improved artificial bee colony algorithm for global optimization," *Inf. Process. Lett.*, vol. 111, no. 17, pp. 871–882, 2011. https://doi.org/10.1016/j.ipl.2011.06.002

[9] C. Ozturk, E. Hancer, and D. Karaboga, "Dynamic clustering with improved binary artificial bee colony algorithm," *Appl. Soft Comput. J.*, vol. 28, pp. 69–80, 2015. https://doi.org/10.1016/j.asoc.2014.11.040

[10] B. Ayyappan and P. Mohan Kumar, "Vehicular Ad Hoc Networks (VANET): Architectures, methodologies and design issues," *2016 2nd Int. Conf. Sci. Technol. Eng. Manag. ICONSTEM 2016*, pp. 177–180, 2016. https://doi.org/10.1109/ICONSTEM.2016.7560946

[11] R. Rahmani and R. Yusof, "A new simple, fast and efficient algorithm for global optimization over continuous search-space problems: Radial Movement Optimization," *Appl. Math. Comput.*, vol. 248, no. December, pp. 287–300, 2014. https://doi.org/10.1016/j.amc.2014.09.102

[12] A. B. Aghababa, A. Fathinavid, A. Salari, and S. E. H. Zavareh, "A novel approach for malicious nodes detection in ad-hoc networks based on cellular learning automata," *Proc. 2012 World Congr. Inf. Commun. Technol. WICT 2012*, no. January 2012, pp. 82–88, 2012. https://doi.org/10.1109/WICT.2012.6409055

[13] K. Adhikary, S. Bhushan, S. Kumar, and K. Dutta, "Hybrid Algorithm to Detect DDoS Attacks in VANETs," *Wirel. Pers. Commun.*, vol. 114, no. 4, pp. 3613–3634, 2020. https://doi.org/10.1007/s11277-020-07549-y

[14] S. Wang, Y. Chen, and H. Tian, "An intrusion detection algorithm based on chaos theory for selecting the detection window size," *Proc. 2016 8th IEEE Int. Conf. Commun. Softw. Networks, ICCSN 2016*, pp. 556–560, 2016. https://doi.org/10.1109/ICCSN.2016.7586584

[15] M. A. Tawhid and K. B. Dsouza, "Hybrid binary bat enhanced particle swarm optimization algorithm for solving feature selection problems," *Appl. Comput. Informatics*, vol. 16, no. 1–2, pp. 117–136, 2018. https://doi.org/10.1016/j.aci.2018.04.001

[16] T. K. Jebuer, "An IDS based on modified chaos Elman's neural network approaches for securing mobile ad hoc networks against DDoS attack," *J. Discret. Math. Sci. Cryptogr.*, vol. 25, no. 8, pp. 2759–2764, 2022. https://doi.org/10.1080/09720529.2022.2075063

[17] V. Bhambhani and H. G. Tanner, "Topology Optimization in Cellular Neural Networks Varsha Bhambhani and Herbert G . Tanner UD MEEG Technical Report Number MEEG TR-2010-0003 Topology Optimization in Cellular Neural Networks," no. July, 2010. https://doi.org/10.1109/CDC.2010.5718073

[18] B. Xu, H. Lin, and G. Wang, "Hidden Multistability in a Memristor-Based Cellular Neural Network," *Adv. Math. Phys.*, vol. 2020, 2020. https://doi.org/10.1155/2020/9708649

[19] A. Cura, H. Küçük, and E. Ergen, "Driver Profiling Using Long Short Term Neural Network (CNN) Methods," IEEE Trans. Intell. Transp. Syst., pp. 1–11, 2020.

[20] J. Q. Kadhim, "Enhancement of Online Education in Engineering College Based on Mobile Wireless Communication Networks and IOT," International Journal of Emerging Technologies in Learning (iJET), vol. 18, no. 02, 2023. https://doi.org/10.3991/ijet.v18i01.35987

[21] H. Tauma, "Secure Chaos of 5G Wireless Communication System Based on IOT Applications," International Journal of Online & Biomedical Engineering, vol. 18, no. 12, 2022. https://doi.org/10.3991/ijoe.v18i12.33817

[22] N. Alseelawi, and H. T. Hazim, "A Novel Method of Multimodal Medical Image Fusion Based on Hybrid Approach of NSCT and DTCWT," International Journal of Online & Biomedical Engineering, vol. 18, no. 3, 2022. https://doi.org/10.3991/ijoe.v18i03.28011

[23] A. H. M. Alaidi, R. a. M. Al_airaji , I. A. Aljazaery, and S. H. Abbood, "Dark Web Illegal Activities Crawling and Classifying Using Data Mining Techniques," International Journal of Interactive Mobile Technologies, vol. 16, no. 10, 2022. https://doi.org/10.3991/ijim.v16i10.30209

[24] H. T. Salim, "Enhanced Data Security of Communication System using Combined Encryption and Steganography," International Journal of Interactive Mobile Technologies, vol. 15, no. 16, pp. 144-157, 2021. https://doi.org/10.3991/ijim.v15i16.24557

[25] T. K. Jebuer, "FINDING OPTIMAL and RELIABLE PATH in MOBILE SINK WIRELESS SENSOR NETWORK by APPLYING GENATIC OPTMIZATION CELLULER NEURAL NETWORK(GO-CNN)," *J. Eng. Sci. Technol.*, vol. 16, pp. 35–42, 2021.

8 Author

Tuka Kareem Jebur she is an Iraqi computer scientist who holds a master's degree in wireless networks from Al-Mustansiriya University. She has many international research papers published in wireless networks and works at Al-Mustansiriya University (email: tukakareem@uomustansiriyah.edu.iq).

Article submitted 2023-02-16. Resubmitted 2023-05-01. Final acceptance 2023-05-01. Final version published as submitted by the author.