Journal of Cyber Security
DOI: 10.32604/jcs.2022.033436
Article

Tech Science Press

Check for updates

An Adaptive BWO Algorithm with RSA for Anomaly Detection in VANETs

Y. Sarada Devi* **and M. Roopa**

DEPT of ECE SRM Institute of Science and Technology, Ramapuram, India
*Corresponding Author: Y. Sarada Devi. Email: sy9149@srmist.edu.in
Received: 21 November 2022; Accepted: 27 December 2022

Abstract: Vehicular ad hoc networks (VANETs) are designed in accordance with the ad hoc mobile networks (MANETs), i.e., impulsive formation of a wireless network for V2V (vehicle-to-vehicle) communication. Each vehicle is preserved as a node which remains as share of network. All the vehicle in the network is made to be under communication in a VANET because of which all the vehicles in the range can be made connected to a to a unit & a wide network can be established with a huge range. Healthier traffic management, vehicle-to-vehicle communication and provision of road information can be done in VANETs. There may exist a possibility that the VANET can undergo attacks or delayed transmission or theft of information. DOS attack, Black Hole Attack (BHA), Sybil attack (SA) can be few among attacks, that may damage the entire network and can cause hammering to life of citizens. Adaptive Black Widow Optimization with Chimp Algorithm (ABWOCA) is used in the paper where in DOS, Sybil and BHA are analysed. Detection and prevention of attacks is the main concentration in the VANETs. RSA algorithm is used for encryption and decryption to the ideal direction-finding, & Enhanced AODV routing protocol (EAODVRP) is designed. The planned technique is realized in the NS2 platform and verified with many affected nodes. The projected technique is associated with the current approaches like Cuckoo Search Optimization (CSO) & Greywolf Optimization Algorithm (GWOA). The statistical parameters like throughput, delay, encryption & decryption time are studied evaluating the performance of the projected technique.

Keywords: VANET; sybil attack; black hole attack; adaptive black widow optimization algorithm; RSA and enhanced AODV

1 Introduction

Vehicular Ad Hoc Networks became prevalent and attractive these days to deliver services such as traffic safety, competence in mobility, navigation, etc. to the end users [1]. VANETs are being extensively used in the ITS to expand conveyance effectiveness, protection and relief in driving. It delivers many non-safeties, safety services for users on road by V2V & V2I communications depending on 2 types of devices: OBU (On Board Unit) mounted on vehicle & RSU (Road Side Unit) sited on side of road. VANET is to rise safety & ease of driver also to manage traffic. V2V communication is

This work is licensed under a Creative Commons Attribution 4.0 International License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

to spread alert info while V2R is to report some happening to the CA (centralized authority) like managing the traffic, response squad in emergency. Timely information will be received from the neighboring vehicles in VANETS to trace the conditions of driving. Periodic exchange of messages about safety will be done amid vehicles which are in communication range to alert the driver. The position and location of the transmitter, velocity of the vehicle, time stamps will be embedded in the packet sent by the initiating node [2].

Conventionally, there may not exist a need of the infrastructure in terms of RSU to establish the communication amid automobile sin VANETs. Nodes in VANET are generally fast in mobility, organized by self which change the topology randomly [1]. Providing authenticity, reliability and integrity of data switched amid OBUs and RSUs are responsible for secure communication, cooperative pre-crash sensing, warning of forward collision and notification of hazard zone. The life of the travelers is one of the important issues, hence, safeguarding VANETs contrary to any kind of attack must be seriously considered. Various attacks in the VANET are: Denial of Service (DOSA) attack, Wormhole Attack (WHA), Black Hole Attack (BHA), Sybil attack (SA), etc. Therefore, the safety matters a lot in VANETs. Sybil Attack is found more dangerous among all the existing in VANETs [1]. Sybil attacks arises when a large number of identities that are not true, try to interrupt the communication amid the vehicles which may straightly affect the facility related to safety of road, congestion of traffic. Sybil attack may be directed in 2 methods: by a balanced attacker to attain self-benefit, or a malicious looking to root damage [1]. In this paper, 3 types of attacks are examined & noticed using ABWOCA (Adaptive Black Widow Optimization with Chimp Algorithm). RSA algorithm is applied for purpose of encryption & EAODVRP (Enhanced routing protocol) is established.

The main contribution of the paper is abridged as below,

- To recognize the several attacks on nodes in VANETs.
- To avoid the Sybil Attack (SA), DoS Attack and Black Hole attacks in VANETs.
- Adaptive Block Window Optimization is industrialized to perceive the attacks in VANETs and protect the network from those attacks.
- The planned procedure is to detect malicious nodes detection and RSA is used for security.
- The proposed method is implemented to circumvent collisions of message & redundancy, such that the lifetime of network is maximized.

The paper is prepared as follows. Section 2 explains the recent associated works are presented. Section 3, presents studies of the network system model on methods to detect various attacks in VANETs using the proposed method. Section 4 presents the performances of the proposed technique by simulation that was performed and Section 6 concludes the proposed technique.

2 Related Works

Every node in the VANET can act as a router depending on the situation and spoofed routing tables can be added by the malevolent node connected to the network because of which the operation of the node can be disturbed. AODV routing protocol was developed by Kumar et al. [3] to overcome this issue to allow the discovery of black hole attack. With all the enhancements in RREP and RREQ packet protocols a new protocol was designed. To improve the level of safety, a cryptography-built encryption and decryption were added to confirm the source and destination nodes. Their method was established using simulator NS-2.33 by means of diverse parameters of network like drop packets, end-to-end delay, packet delivery ratio (PDR) and routing request overhead. Outcomes validated that

the projected technique outdoes current routing protocol, AODV with black hole attack & improved the performance of network.

Iwendi et al. [4] projected a geographically stimulated spider-monkey time synchronization method for significant VANETs to increase packet delivery time consuming lowest energy. The technique proposed was constructed on the metaheuristic inspired outline by the natural spider-monkey performance. A method artificial spider-monkey was considered to test the attacking tactics (Sybil) on VANETs to forecast the count of collisions amid vehicles in a tightly positioned trial zone. A comparison was made amid the newly designed and existing protocols and found that the proposed system acts better over long-distance transmission with respect to precision measurement, energy efficiency and rate of intrusion detection.

Determination of the harmful nodes can be made by sending malevolent data or considerable packets to the vehicles or RSU (Road Side Unit). To forgo this, Kolandaisamy et al. [5] has established a SPPA (Stream Position Performance Analysis) method. Their method observed the location of any node in transmitting the data to make a Distributed Denial of Service (DDoS) attack. Their technique calculated numerous issues with respect to data being transmitted, and sample rate. The trustworthiness of the data transmitted is identified and is included in making decisions. This method improved the detection performance of a DDoS attack in the VANET.

Among all the attacks faced by VANET Sybil Attack (SA) was found to be more dangerous. Manifold identities are generated by the attacker to false nodes. To defend and detect is extremely burdensome especially genuine identities are used. A technique CMEHA-DNN was developed by Nitha C. Velayudhan et al. to detect the SA in VANET with 4 stages: (i) Cluster Development (CF) (ii) Cluster Head (CH) collection (iii) attack discovery and (iv) providing safety.

Protection against attacks like GHA (Gray Hole Attack) and BHA (Black Hole Attack) was carried out using ANN by Pooja Rani et al. [6] as an algorithm in deep learning using the swarm-based ABC (Artificial Bee Colony) optimization method. The performance of the system was amplified by selecting suitable and finest nodes for transmission of packets. MATLAB software was used to design the network and simulation with neural network and communication toolboxes. The results inspected display that the offered protocol performed healthier in disparity to the existing under gray hole as well as black hole attacks.

An IDBA (intelligent black hole attack detection) system was personalized to ACV by Hassan et al. [7] considering four key limitations in the project, viz., Packet Delivery Ratio (PDR), Hop Count, Destination Sequence Number, End-to-End delay (E2E) and verified the presentation of IDBA in contradiction to BAODV, IDSAODV & EAODV algorithms. Extensively, results after simulation showed that IDBA outdoes current methods in terms of E2E, PDR, Packet Loss Rate, Routing Overhead and Throughput.

Quite a few investigators worked to detect and justify numerous attacks. But the fortification of VANET in contradiction to multiple threats is threatened. Hence, in this paper, 3 types of attacks are examined with the utilization of Adaptive Black Widow Optimization with Chimp Algorithm (ABWOCA). For the encryption analysis, RSA algorithm is applied and Enhanced routing protocol (EAODVRP) is industrialized. The featured explanation of the planned procedure and model of the system are defined below.

3 VANETs System Model

In the section, the system architecture of VANET is as shown in Fig. 1. Different attacks are identified by making use of the algorithm proposed. Fig. 1 explains the method in which the vehicles are connected to RSUs'. In Fig. 1, it can be observed that messages are being transmitted to the RSU from vehicles which can be helpful for detection of the position (which will be stored in one of the RSUs') of the vehicle from which message is transmitted. Each vehicle is armed with OBU which stores the thorough data like speed, position about the vehicles. VANETs have extensive application abilities in the ITS like traffic organization, avoidance of accident. However, security has always been a contest whose loss might cause destruction to ITS.

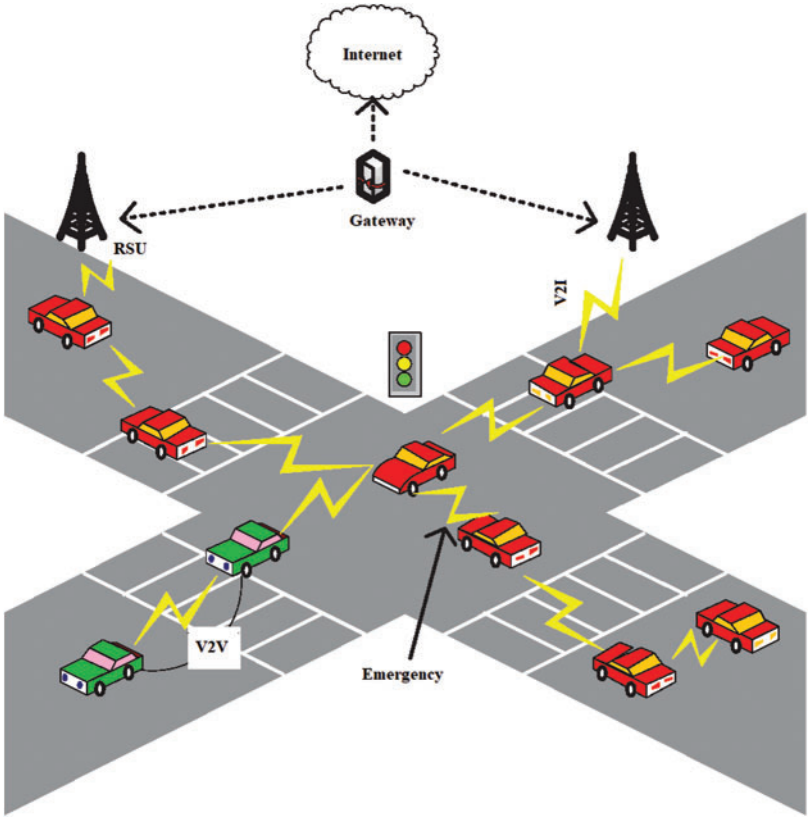

Figure 1: VANET architecture

3.1 Attacks in VANETs

3.1.1 DOS

DOS attacks are because of the [8] network outsiders and insiders leaving network unavailable to physical users by flooding the control channel. As a result, RSU and OBU will be incapable to progress in a full-fledged manner. The system with DOS Attack is illustrated in the Fig. 2.

From the above figure, the car C is an attacker and car B, D, E, F, H are affected by DOS attack.

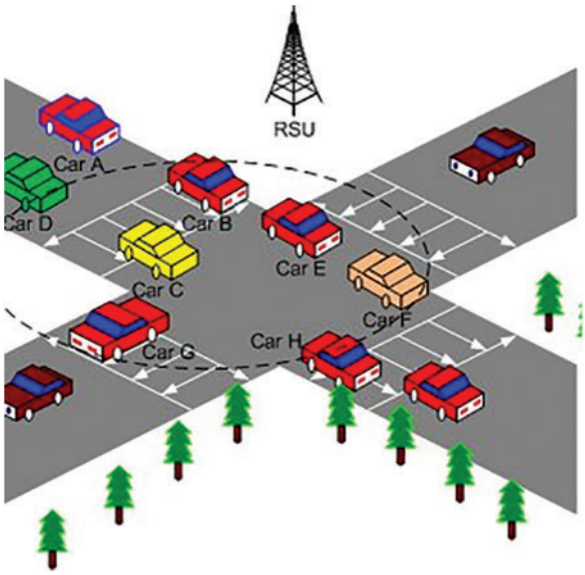

Figure 2: Structure of DOS attack

3.1.2 BHA in VANETs

Concerning safety, a Black Hole Attack is such risk in which the data packets or control are released from the malevolent vehicle, changing a harmless connection to a negotiated one. Performance of VANET's is severely affected by dropping data packets which may root for loss of life, accidents & traffic jams. In this paper, ABWO based EAODVRP is applied to notice and stop the BHA in VANETs. By using the planned technique, BHA is noticed at a primary phase grounded on the route discovery process, which is helpful to progress on the security of system. The projected explanation is grounded on calculating a self-motivated value of threshold and producing a fake request for route (RREQ) packet. In the Fig. 3, the BHA design is exemplified which stipulates the access point, RSU, attacker's node & route detection track.

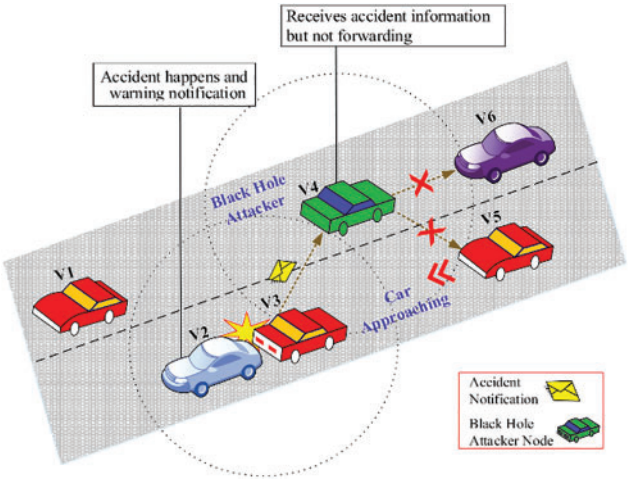

Figure 3: Black hole attacks in VANETs

3.1.3 SA in VANETs

The identity of multiple vehicles is forged by this attack [9]. These characteristics are used to any kind of attack onto system. These incorrect characteristics generate an impression that there can be added vehicles on road and takeoff the locations of other nodes in the network. Sybil attack is measured as a thoughtful safety hazard to VANETs meanwhile, disseminating the false messages using numerous forged characteristics to attack innumerable applications of ITS. Discovery of Sybil nodes is a well-organized system in contradiction to Sybil attacks, which will adopt location approximation, delivery confirmation or resemblance judgement to recognize Sybil nodes. Inaccurate location of th nodes can take place when there exist deliberate changes in transmission of power between sybil nodes. Thus, it is highly problematic to distinguish normal from Sybil nodes via normal RSSI approaches.

3.2 Strategy for Prediction of Attacks in VANET

The planned routing procedure for VANETs, offers the require route based on request. The node at the receiver verifies the keys and the message is not transmitted as usual. The messages being transmitted and received will be highly secured by using the proposed method by using encryption and decryption techniques of RSA algorithm. Providing authentication is a prime factor in RSA. Authentication at the receiver will be done by Rumour riding process which has various queries to be answered. If the receiver answers the queries correctly the key will be transmitted else its concluded to be attacked by a malicious node. The process of routing will be enabled using the proposed method routing will be progressed. It can simply be concluded that to establish routing between nodes authentication must be done using RSA method followed by RREQ strategy.

The nodes which intend to transmit the data should register in the network along with the opposite route information. Count of number of hops, end time of the route identification of nodes, the sequence number source, the destination & source identifier are to be updated regularly in the network. The path of the transmission in a particular path will be prominent only when the sequence number of the node is approved. The node then transmits a RREP, with info in the path conflicting to the node that is transmitting data. Finally, the procedure involved in the proposed algorithm is explained below.

The message to be transmitted is encrypted using RSA algorithm and the data is sent to the neighbouring node after getting aware of the status of the node after authentication. By means of the planned method, the tainted RSU is recognized and detached from the network. The attack node & despoiled RSU are recognized that can breakdown the performance of the system. Hence, the malevolent RSU is detached from the network while the communication goes on. The key which is encrypted is made to move between the nodes in the 2nd step. This process of continuously validating the route and using a key is validated in every loop of the transmission in 3rd step. Lastly, when the neighbouring node is found harmless the key which has to be kept secret is transmitted between nodes. So, the validation is to be completed amid request & response type that packet is conveyed. Three varieties of attacks are identified using the use of proposed protocol & command script.

As the designated node is established using routing table, the identity of the node will be validated, depending on the digital signature, that's known previously. Moreover, the nodes should compute hash for data to be transmitted, which allow nodes to authenticate the honesty of data to run the same hashing algorithm used to compare the hash to the locally designed.

The demanded node directs an enquiry to neighbouring nodes to fold the essential resources. When initiating node turns as a malicious node, it makes a false appeal & introduces fake search resources [10]. The answering node acts to be malicious, which transmits an identical response to source node. The conditions of different attacks are as in Figs. 2–4.

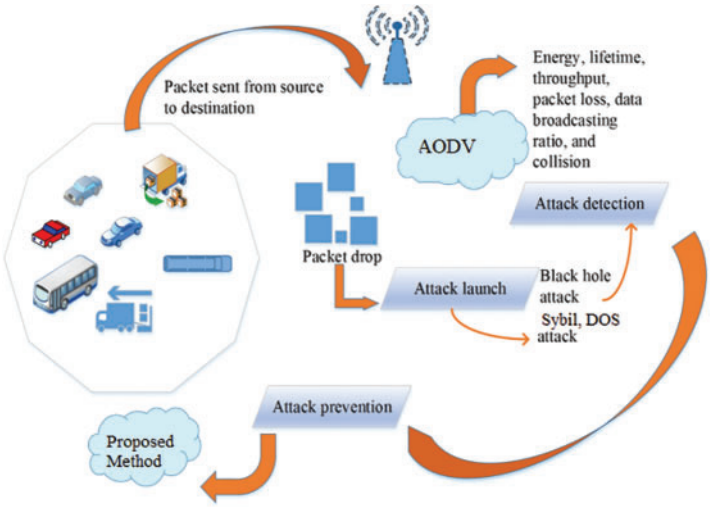

Figure 4: Proposed method for attack detection in VANET

The position of every node can be gained reliant on the condition, and the mandatory resources are composed from neighbour in the VANET network. The location, IP address with rate of success can be allocated built on previous communications to every node in original state, which will help in identifying the status of each node. The performance of the system can be analysed by using rumour riding technique. The neighbour node is designated built on value of probability which measured as initial collection of nodes for rewarding essential resources. To identify the attacker node or safe node scenario designated node can be tested with proposed technique. The detail description of attack detection is described in the pseudocode.

Pseudocode:

Initialize: Number of parameters, Vehicles
If (S receives a data)
RT of S is checked to form route to D
If (S takes a dynamic route in RT)
The data has to be sent to nest neighbor to D
Else the route discovery process should be started by transmitting
If (PREQ message will be received by I or D)
The PREP will be initiated by I if an active route is found for D
or
The PREP message is initiated by D initiates in which some PREQ/ELSE is acknowledged by A
A PREP message will be created and will be left as reply from A with sequence number matching to D
End If
If (the PREP is received with valid & D_{seq} by S)
A route is created for D by S with A as an I in it
The novel route revealed can be used to transmit the data
A data packet is dropped without being forwarded when a data packet is retried by A

(Continued)

Pseudocode: Continued

```
            End
        End
End
```

RSA Algorithm

Public and Private keys are involved in RSA. Following methods in Fig. 5 explains how the keys are generated.

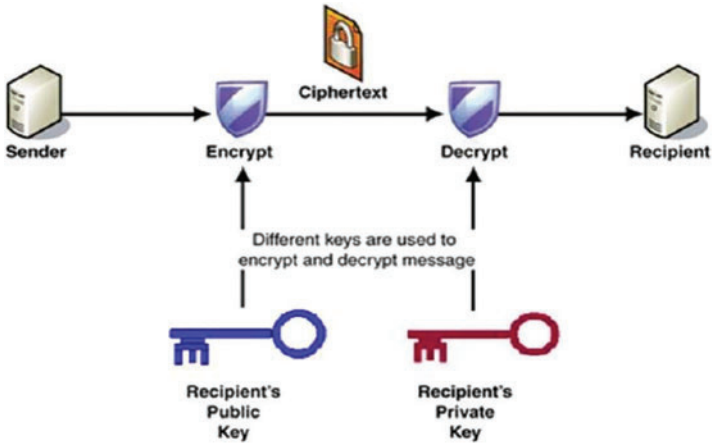

Figure 5: RSA algorithm

Security of data along with its identity can be well maintained using RSA algorithm. This can enable the privacy of the vehicle location in VANETs. BWO is used to choose best key assortment operation. BWO algorithm is in detail given below.

3.3 Process of Black Widow Optimization

The projected procedure of BWO is applied to discover the best way & provide security VANET. Node, energy and detection rate of attack are the input to algorithm. To achieve the ideal case, limitations are adjusted by means of BWO algorithm. In this section, a detailed description of BWO and the proposed algorithm are offered.

3.3.1 Black widow optimization

Following are considered as the basic features of cannibalism which is the main stage in BWO.

Initial population

The inputs to the BWO algorithm are random keys and attack nodes as measured by a black widow spider which is treated as a separate limitation. The following is the formula for the BWO's initial population:

$$W = \left[X^1, X^2, \ldots, X^{N^{Var}}\right] \tag{1}$$

where, N^{Var} can be denoted as the dimension of constraints, X^1, X^2 may be denoted as numbers in floating-point obtained using fitness function which is described as below,

$$F(W) = f\left[X^1, X^2, \ldots, X^{N^{Var}}\right] \tag{2}$$

The best weighting limit of node is adjusted optimally based on fitness function. Efficient process can be enabled by maximising the efficiency of the node and minimization of error. The fitness function is attained by choosing the ideal value of weighting parameter. Mathematically, the fitness function is expressed as:

$$\mathrm{FF} = (Max\,(EE^n)) \tag{3}$$

The matrix is constructed using a chance generator and an extended as widow array. The procreate is formulated as follows, based on descendant's operation:

$$\begin{cases} v^1 = \mu * z^1 + (1-\mu) * z^2 \\ v^2 = \mu * z^2 + (1-\mu) * z^1 \end{cases} \tag{4}$$

This technique can be repeated with different numbers at different times that are unlikely to be replicated. Finally, the array can be organized by metrics and rating.

The termination state can be evaluated with the three processes, similar to previous algorithms: (1) attainment of stated degree of correctness, (2) no difference in value of fitness and (3) multiple iterations. This is useful in various standard optimization problems since it allows for the collection of optimal solutions. The termination situation was also examined. Optimal routing is selected and security is given by the projected technique. Fig. 2 Gives the entire process of proposed method. The entire procedure of the BWO algorithm is given the flowchart of the BWO is shown in Fig. 6:

Procedures:

- The population under the black window are initialised and a key is generated at random.
- Key generation, initial parameters and maximum iteration are selected.
- The fitness value is computed, random key generated is engaged as fitness function. In this projected BWO algorithm.
- The boundary settings cannibalism is computed for behaviours of black widow.
- For the Security purpose, the random key is generated and the encryption and decryption are achieved with the help of RSA.
- ❖The position of spiders is updated, Based on the distance.
- The conditions of boundary are checked for black widow & optimal routing and key are computed with proposed algorithm.
- The algorithm is made immobile when it reaches the extreme iteration & optimal results are found optimal.

From the above it can be understood that, computation of RSA (key) is done based on the fitness function with which the security of the system can be increased. The privacy of location in VANET can also be enabled with this technique.

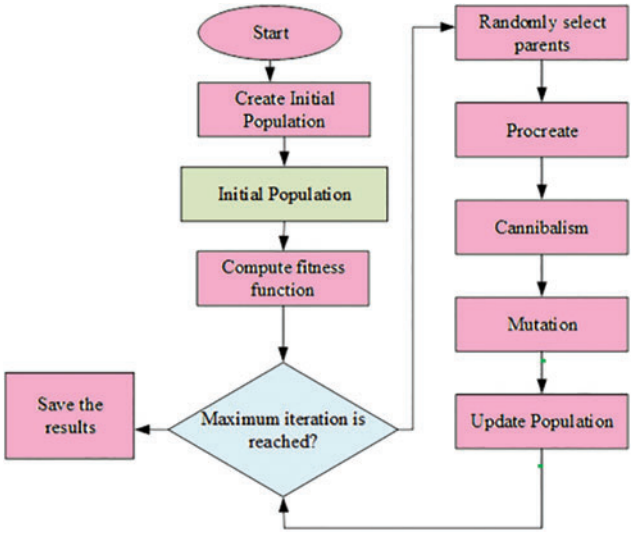

Figure 6: Flowchart of the BWO

4 Results and Discussions

In the segment, the detection of attack in VANETs is examined and applied on operating system (Ubuntu) with a simulator-NS-2.33. Table 1 lists all the parameters considered for simulation. Random generation of nodes is done with 100 along with malicious nodes. Figs. 7a and 7b, respectively gives original and last situations of experiments. Numerous parameters of network are assessed to analyze the performance. Fig. 7b illustrates the effect of nodes that are malicious. PDR is found to decrease with a rise in malicious nodes. The overall performance is observed to be degraded with drop in the RREQ packets which further increases the ration of packet loss.

Table 1: Implementation parameters

S. No	Description	Constraints
1	Number of vehicles	150
2	Vehicle velocity	11–35 m/s
3	Packet size	500 Bytes
4	Channel model	Channel/WirelessChannel
5	Prop	Propagation/TwoRayGround
6	netify	Phy/WirelessPhy
7	MAC	Mac/802_11
8	Simulation area	1000 m $*$ 1000 m
9	Rate	100 kb
10	Road side unit	20 m/s

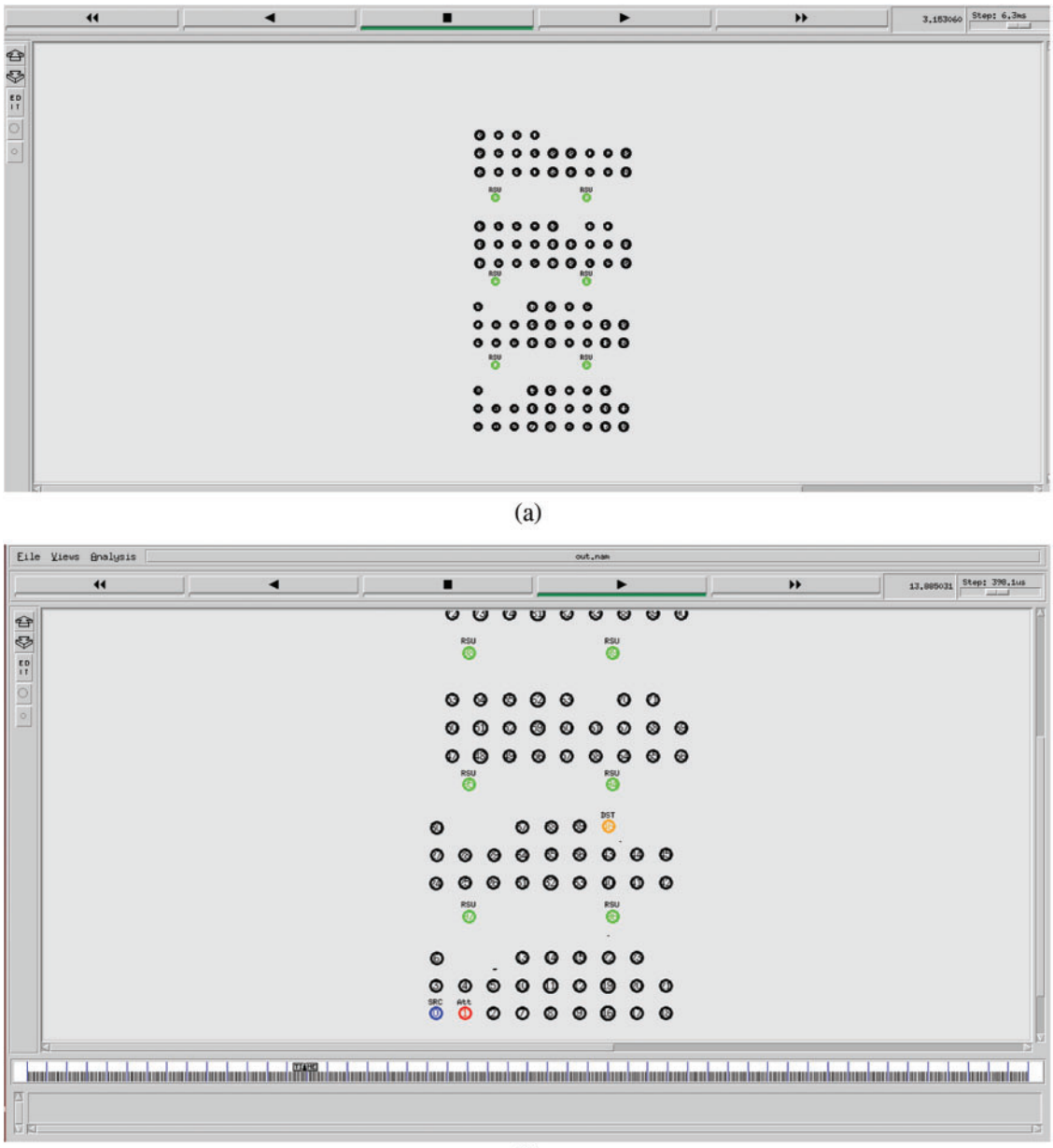

Figure 7: Illustration of (a) Node initialization and (b) Attacks node

As shown in Fig. 8a. Different circumstances are considered for the comparison of throughput. Comparison of the novel method is done with the prevailing approaches CSO & GWO for numerous malevolent nodes in the absence/presence of attacks (Sybil, Blackhole, DOS). The typical throughput of approach, proposed, is 3540 kbps, whereas its 2210 & 3020 kbps for CSO & GWO respectively.

In the below Fig. 8c shows that the delivery ratio is evaluated under the various vehicles. Here vehicle variation is denoted as the node variation. The delivery ratio is compared with existing methods like GWO, CSO for various nodes malevolent in the absence/presence of Sybil, DOS, Blackhole

attacks. The delivery ratio (average) of the projected method is 68 s, but the current method has a delivery ratio 75.6%. In contrast, the delivery ratio of the existing method has 66.4% and 62.8%. Similarly, the network life time and delay are analyzed and compared with the proposed method.

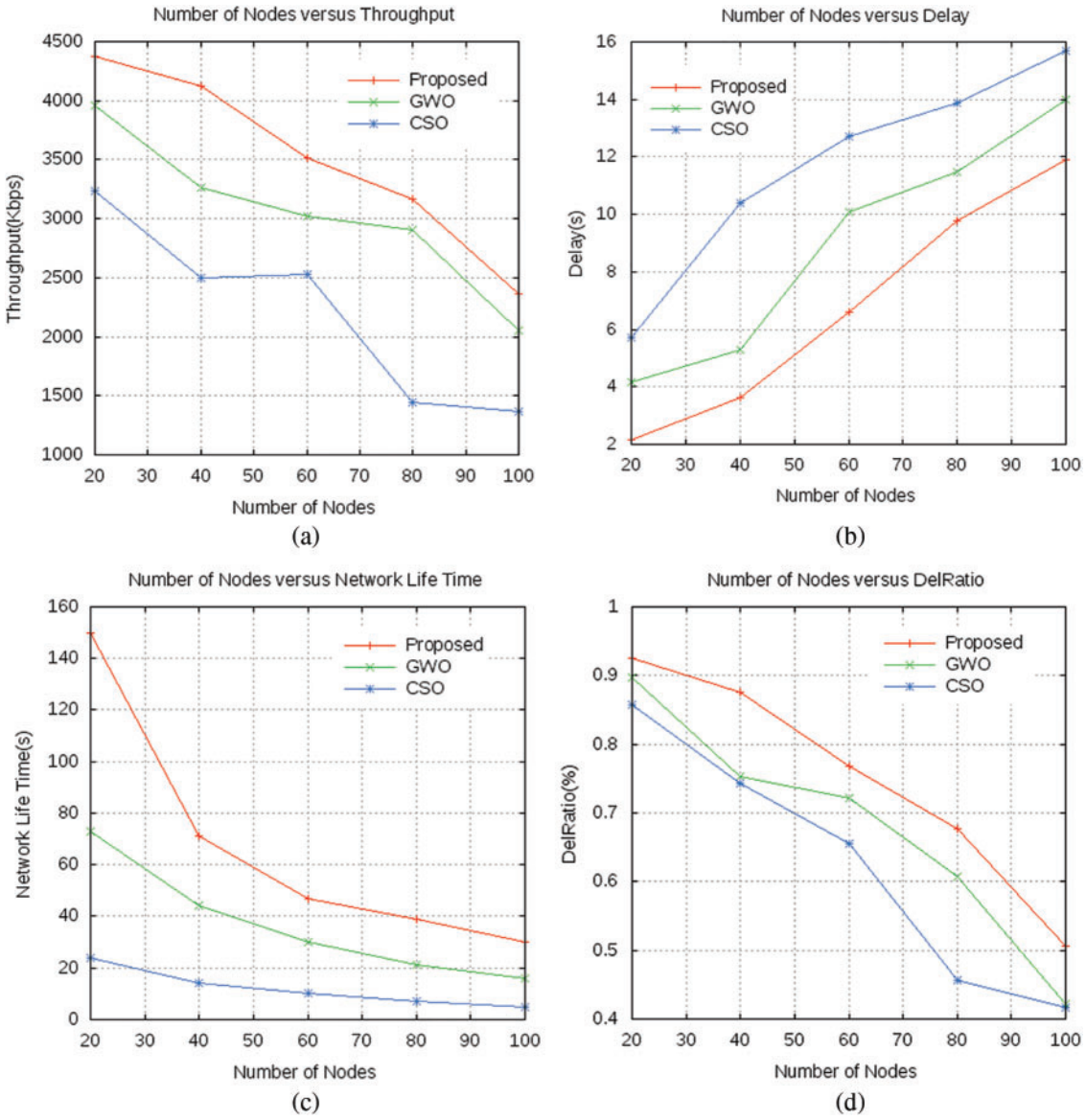

Figure 8: Comparison analysis of (a) Throughput (b) Delay (c) Network life time and (d) Delivery ratio

Fig. 9 shows that with upsurge in speed of Nodes the malicious node may not be capable of capturing all packets with RREQ produced as the nodes with more speed may move out of network in no time resulting to decrease in Packet delivery ratio.

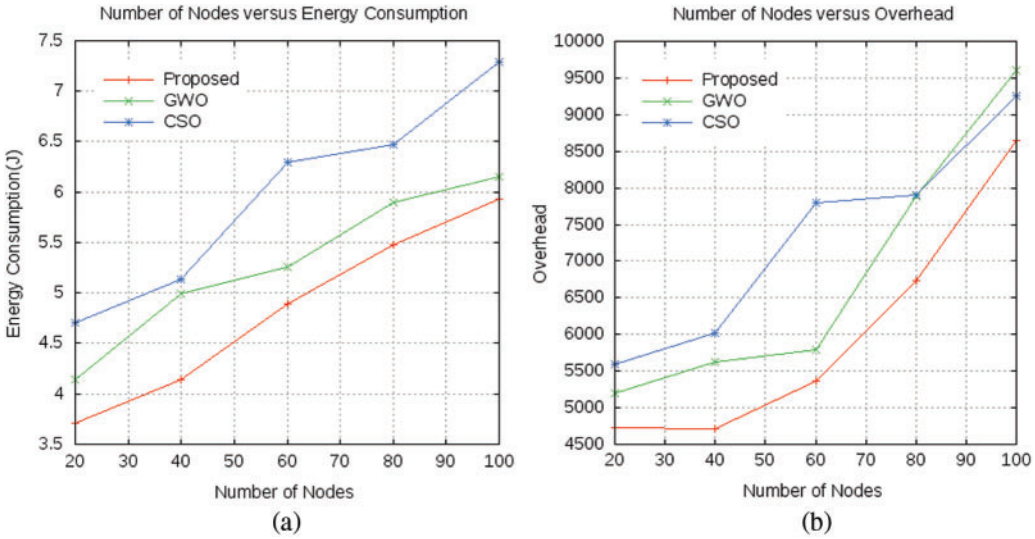

Figure 9: Comparison analysis of (a) Energy consumption and (b) Overhead

From the below Fig. 10, the encryption and decryption time is illustrated. For the secure operation, the RSA algorithm is used to generate key for encryption and decryption. Here, the proposed method has less time for encrypt and decrypt the values. But, in other methods, it shows high for encryption and decryption process compared with the proposed method. From the Fig. 10b, the projected technique has the time of encryption 110 s with the existing methods as GWO and CSO have the encryption time is 122 and 138 s respectively. Fig. 10a labels the time for decryption of existing & proposed approaches. From the analysis, the projected method, GWO, CSO methods have the decryption time of 30, 36, 39 s respectively. The study guides to conclude that the projected technique has less time of encryption and decryption which increases the system performance when compared with the prevailing methods.

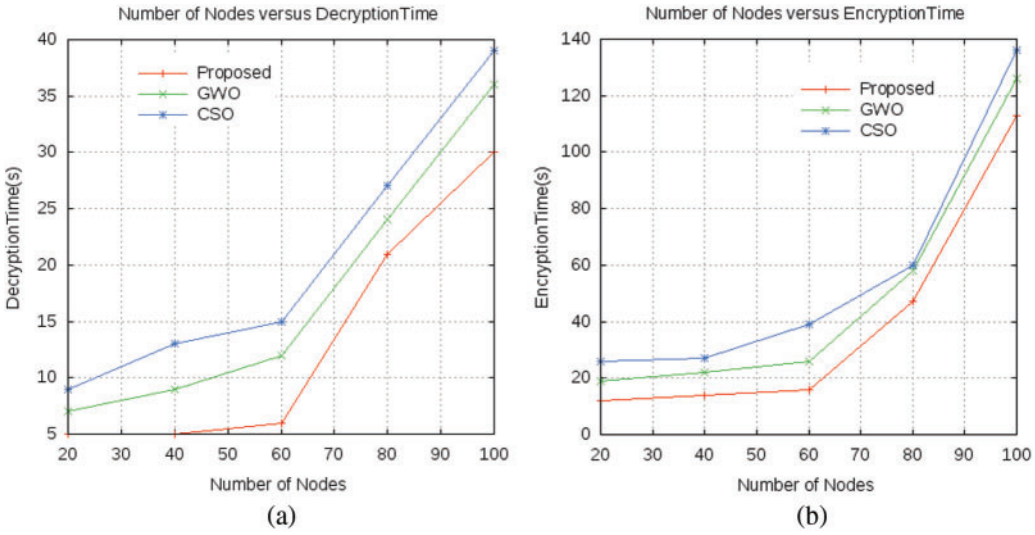

Figure 10: Comparison analysis of (a) Encryption time and (b) Decryption time

In Fig. 11, the attack detection ratio is analysed by using various methods. In the Blackhole attack detection, the detection rate 95% is achieved by using the proposed method and the other existing methods are achieved as 84% and 72% respectively. Similarly, the anticipated process has attained 96% rate, 93% rate, for DOS attack and sybil attack respectively. By using other methods has the detection rate is 83%, 70% and 76%, 78% respectively. The study gives that, the proposed methodology is realized finest detection rate for blackhole, dos, and sybil attack detection and detection rate.

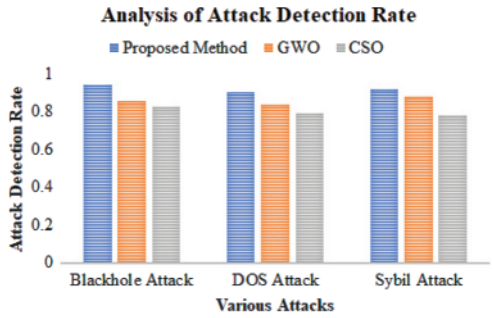

Figure 11: Comparison analysis of attack detection rate

By overall study, it's found that the projected method is utmost important part, to demonstrate competence of the projected method compared with the prevailing methods. The projected method for detection of Blackhole, DOS and Sybil attack in VANETs networks can be attained using proposed system. A query can be sent to another node on request and this request is forwarded to the neighboring nodes requesting resources. Forwarding the queries and waiting for resources between all the nodes may take longer time which has to be reduced by balancing the load and enhancing the security. The comparative study of method proposed is examined with metrics of performance like delivery ratio, delay, packet loss and throughput and the results were found much better in the proposed technique when compared with the existing.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] S. RoselinMary, M. Maheshwari and M. Thamaraiselvan, "Early detection of DOS attacks in VANET using attacked packet detection algorithm (APDA)," in *2013 Int. Conf. on Information Communication and Embedded Systems (ICICES)*, Chennai, India, IEEE, pp. 237–240, 2013.

[2] Y. Yao, B. Xiao, G. Yang, Y. Hu, L. Wang *et al.,* "Power control identification: A novel sybil attack detection scheme in vanets using rssi," *IEEE Journal on Selected Areas in Communications*, vol. 37, no. 11, pp. 2588–2602, 2019.

[3] A. Kumar, V. Varadarajan, A. Kumar, P. Dadheech, S. S. Choudhary *et al.,* "Black hole attack detection in vehicular ad-hoc network using secure AODV routing algorithm," *Microprocessors and Microsystems*, vol. 80, no. 3, pp. 103352, 2021.

[4] C. Iwendi, M. Uddin, J. A. Ansere, P. Nkurunziza, J. H. Anajemba *et al.,* "On detection of Sybil attack in large-scale VANETs using spider-monkey technique," *IEEE Access*, vol. 6, pp. 47258–47267, 2018.

[5] R. Kolandaisamy, R. M. Noor, I. Kolandaisamy, I. Ahmedy, M. L. M. Kiah *et al.,* "A stream position performance analysis model based on DDoS attack detection for cluster-based routing in VANET," *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, no. 6, pp. 6599–6612, 2021.
[6] Pooja Rani, Kavita, Sahil Verma and Gia Nhu Nguyen, "Mitigation of black hole and gray hole attack using swarm inspired algorithm with artificial neural network," *IEEE Access*, America, vol. 8, pp. 121755–121764, 2020.
[7] Z. Hassan, A. Mehmood, C. Maple, M. A. Khan and A. Aldegheishem, "Intelligent detection of black hole attacks for secure communication in autonomous and connected vehicles," *IEEE Access*, vol. 8, pp. 199618–199628, 2020.
[8] S. Zeadally, R. Hunt, Y. S. Chen, A. Irwin and A. Hassan, "Vehicular ad hoc networks (VANETS): Status, results, and challenges," *Telecommunication Systems*, vol. 50, no. 4, pp. 217–241, 2012.
[9] M. Rahbari and M. A. J. Jamali, "Efficient detection of Sybil attack based on cryptography in VANET," arXiv preprint arXiv:1112.2257, 2011.
[10] G. Hu, B. Du, X. Wang and G. Wei, "An enhanced black widow optimization algorithm for feature selection," *Knowledge-Based Systems*, vol. 235, no. 7, pp. 107638, 2022.