I. J. Computer Network and Information Security, 2021, 2, 39-52
Published Online April 2021 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2021.02.04

Secured Message Broadcasting in VANET using Blowfish Algorithm with Oppositional Deer Hunting Optimization

M. Selvi
Research Scholar, Department of computer science, S.T. Hindu College, Affiliated to Manonmaniam Sundaranar University, Tirunelveli.
E-mail: selmca@gmail.com

B. Ramakrishnan
Associate Professor, Department of computer Science, S.T. Hindu College, Nagercoil
E-mail: ramsthc@gmail.com

Received: 18 November 2020 ; Accepted: 13 January 2021; Published: 08 April 2021

Abstract: Emergency Message broadcasting is an important process in VANET. Security and reliable transmission are the two major concerns in message broadcasting. VANET is open to unauthorized nodes, hackers, misbehaving vehicles, malicious attackers etc without security. Without valid confirmation of authorized vehicles, these types of attacks may occur. To enhance the reliability in message broadcasting, some existing techniques are used. They transmit the data without much delay but they didn't provide any trusted authentication. So hackers, malicious nodes, unauthorized vehicles may easily interrupt the emergency messages. Also Brute force attack, Man in Middle attack are not identified and eliminated. In this research, a trust based secured broadcasting mechanism is developed which ensures the metrics such as security, privacy, integrity, trust etc. The major intension of this research is to reduce latency and provide high reliable, secure and efficient communication over the vehicles. The data such as vehicle position, location, speed, and other traffic information's are generated and stored in a separate table. A network is created with varying densities. A path is generated for message broadcasting between source and destination based on the specific gateway estimated. Here, Optimal Wireless Access in Vanet (OWAV) Protocol is employed to gather vehicle related information to reduce the delay. Blowfish encryption algorithm along with Oppositional Deer Hunting Optimization (ODHO) is used to store the trusted vehicles location to avoid unauthorized tracking. The performance of the proposed research is analyzed with various metrics such as Packet delivery ratio (PDR), transmission delay, encryption time, throughput, computational overhead etc. The efficiency of the research is compared with other existing methods.

Index Terms: VANET, Security, Active and Passive attacks, Deer Hunting Optimization (DHO), Oppositional behaviour learning (OBL).

1. Introduction

Vehicular information Broadcasting or message dissemination process is a promising research topic in recent days. The most important issue on this broadcasting process is the detention of the routing problem to vehicle to vehicle (V2V) scenarios as opposed to wireless communication [1]. In a primary scenario, security and transport proficiency is an order for current vehicle producers and this must be given by the vehicles out and about instead of likewise utilizing the current wireless communications foundation, such applications with these true limitation requires another steering convention for vehicular broadcasting in VANET [2, 30,32]. Secured data transmission empowers life-basic applications, for example, the alarming usefulness during crossing point navigating and lane integration, and in this manner, assumes a key part in VANET applications [3, 4]. The communication between vehicle to vehicle (V2V), vehicle to road side unit (V2I) done through wireless communication which is the major cause for security in vehicular transportation applications [1].

VANETs features lot of security obstacles and issues associated to authentication and privacy [22–26]. Notwithstanding these, unauthorized vehicles raise numerous security and communication issues in VANETs [12]. Vehicular network are more vulnerable to attacks and privacy issues because of it open access nature. In this manner, the hacker can adjust, block, infuse, and erase the messages in VANETs. For instance, the unauthorized person can get the admittance to the traffic messages, which are utilized to direct the vehicles out and about. The assailant may adjust these messages and may spread bogus data out and about, which causes gridlocks, traffic occurrences, hazards, mishaps,

risks, and so forth.

So as to successfully relate VANETs in remote communication, safety and protection issues must be taken care of proficiently by employing the efficient algorithms in order to deal with different types of security threats. To solve these problems, a few research methods have been proposed regarding confirmation and security plans for the VANET framework. A couple of techniques utilized "Public key infrastructure (PKI)" [31] plans to approve vehicles, which contain the digital signature of the certification authority (CA) and vehicles' open keys. Hence, the vehicles and RSUs require a ton of computational time and memory to measure and affirm these affirmations [27,28]. These plans make progressively strong arrangements by confirming marks of every vehicle. Notwithstanding, it makes two issues [25].

In security and privacy consideration the most important thing is message authentication. For doing it appropriately and effectively, it should seek after the security requirements for example confidentiality, authentication, integrity and privacy to shield against the hackers and malevolent vehicular hubs [11]. There are lot of attacks for instance black hole, Sybil, DoS, Timing, Illusion etc. that are not only involve the privacy of drivers and vehicles but also compromise traffic safety and can direct to thrashing of life. Consequently, with the intention of turn out to be a real technology that guarantee traffic safety VANETs have need of proper security techniques and mechanisms that will assure protection against different misbehaviours and malicious nodes that concern security of VANET [6-9].

Against malicious attacks and hackers, it is necessary to seek metrics such as privacy, non repudiation, confidentiality, authentication etc for secured message broadcasting. So many attacks available in VANET such as DoS, MiM, black hole, Sybil, in which they are not only interrupt the driver’s privacy but also the entire network traffic [10]. So the main objective is to develop an efficient technique to guarantee traffic safety and quality of service security metrics in VANET which give protection against misbehaviours and attacks.

In this research, optimal encryption technique is used to ensure the broadcasting security. The organisation of the paper is as follows. Section 2 presents the review of recent researches and problem identified. The proposed research is described in section 3 with block diagram and pseudo codes. Section 4 represents the performance analysis and discussion with other existing works. Finally concludes the research in section 5.

2. Literature Survey

As of late, various overviews on VANETs have been proposed identifying with security and protection plans. These overviews secured most parts of VANETs, yet with constrained coverage on VANET security benefits alongside the latest strategies. In any case, there is an incredible need of a far reaching review that dissects the VANET security and protection issues from alternate points of view and fills the limitations of the above studies.

In VANET, the security is most needed one for message broadcasting, hence in this survey the recent techniques available in message broadcasting security is analyzed.

Security in vehicular network guarantees that the forwarded information are not infused or changed by the hackers. Moreover, the driver is answerable for advising the traffic setting precisely inside the restricted time span. Vehicular networks are extra perceptive to the hackers due of its unique features. In particular, security difficulties ought to be tended to appropriately; else, it will make numerous requirements for secure communication in VANETs [29]. The fundamental security parameters are classified as, data integrity, availability, authenticity, non-repudiation, and confidentiality.

Shiang-Feng Tzeng et al. [12] have been proposed the improving security and privacy for consignment authentication scheme in VANET. The author proposed modified “identity-based batch verification” (IBV) scheme. It has three phases. In the system initialization phase, TA generates and preloads the system parameters for all RSUs and vehicles. The identities of anonyms, neighbouring RSU, vehicles in the unknown identities and message signing phases were generated by using tamper proof device. In message verification phase the node ensures the unloading data. This was preferable for both V2I and V2V communication.

Shrikant Tangade et al., [13] have been proposed the VANETs secured authentication scheme based on scalability and decentralization. The architecture of this model contains two layers such as Master Trusted Authority (MTA) and Agents of Trusted Authority (ATA).The top layer of MTA contains communication components these are secured with wired or wireless channel. An ATA acts as a bottom layer; this layer contains two communication components (i.e.) RSUs and OBUs. In the network the MTA was assumed to be powerful and highly trusted components. The main aim of MTA was to create master private, public, and secrete keys. In this work the DSPA scheme was reduced the overheads of computation and communication.

Muthu meenakshi R. et al., [14] have discussed about the extended 3PAKE authentication scheme for analysis of the security and performance issues of VANETs. The author was introduced vale added scheme for avoiding some problems such as confirmation failures, Attacks, routing overhead, transmission delay etc. It was also enhances the service deliveries efficiency by applying a group message transmission method. The introduced scheme provides faster response to the proficient prioritizations of the requirements. In their work, the performance was analyzed with various metrics such as delay in confirmation, delay in service response and routing overhead etc. The communication overhead of the scheme was reduced during packet exchanging by the performance of the schemes. In quick responses the delay metrics was minimum. But it was not preferable for other evaluation such as security over attacks during

communication.

Broadcasting is a significant barrier of VANET. It is the utilization of remote communication for sharing data among nodes and framework. Broadcasting is the primary communication crude in vehicular systems administration for two fundamental reasons, practically all VANET applications need to have a similar snippet of data with numerous vehicles in some zone and furthermore for multihop dispersal most approaches depend on different forwarders. Periodical broadcasting of emergency messages containing the data of area, speed, information about header, and braking status of every vehicle, can empower a wide assortment of advanced VANET applications. Being refreshed with such data, drivers can set aside activities in effort to maintain a strategic distance from potential risks.

Falko Dressler et al., [15] have discussed about a holistic network layer for VANETs. These layers are a new, incorporated, transmission based Network layer. The author creates a four broadcast classes that address all known applications. In class A protocols that broad cast messages based on periodic routine to nearby vehicles, Present process of vehicles also informed to every node. In class B protocols broadcast emergency events but only few vehicles data are detected. The certain specific geographic region information was disseminated using geo-routing and reliable broadcasts in class C. These layers are based on the detecting node location to reads data on the occasion and makes decision forwarding. Time and whether condition about the event has been obtained. Non urgent events are disseminated by using class D protocols.

Feukeu E.A., et al., [16] have proposed the "Dynamic Broadcast Storm Mitigation Approach (DBSMA)" for VANETs to avoid the broadcast storm problem. In their work cooperative awareness is done by CAM type message. The "Channel Busy Ratio (CBR)" measure thought was designed to evaluate the effectiveness of DBSMA. Implementation of DBSMA was simple and easy.

Daxin Tian et al., [17] have discussed about the broadcasting an emergency messages in VANETs. Among the large scale vehicle networks message dissemination was obtained by improved position-based protocol. This protocol is designed for both urban and highway scenarios. The message broadcasting will be done by the input message received by the vehicles and the next decisions taken based on the data packet received in order to avoid further delay or congestions. With a help of ROI the data are transmitted and minimized the collisions and unwanted retransmissions.

The conventional cryptographic algorithm has high time complexity and inefficient in handling all types of attacks such as MiM, Sybil attack, DoS, Brute force etc. The existing researches only covered limited security threats and attacks and this leads to develop an efficient technique which includes all the five security parameters and reliable data transmission with less communication overhead.

2.1. Objectives of the research

Security and privacy are two critical issues on Vanet message broadcasting. In our research, the most important security parameters availability, confidentiality, data integrity, authentication and non repudiation are solved using efficient cryptographic algorithms.

This research intends to:

- Design an optimal cryptographic algorithm and develop a secured vehicular message broadcasting system.
- Design a vehicular authentication scheme conciliating all the five security parameters such as availability, confidentiality, data integrity, authentication and non repudiation.
- Analysis with various passive and active attacks to ensure the effectiveness.

3. Proposed Method of Secured Message Broadcasting in VANET

The major intension of this research is to reduce latency and provide high reliable, secure and efficient communication over the vehicles. The data such as vehicle position, location, speed, and other traffic information's are generated and stored in a separate table. A network is created with varying densities. A path is generated for message broadcasting between source and destination based on the specific gateway estimated. Here, Optimal Wireless Access in VANET (OWAV) Protocol is employed to gather vehicle related information to reduce the delay. Blowfish encryption algorithm along with Oppositional Deer Hunting Optimization (ODHO) is used to store the trusted vehicles location to avoid unauthorized tracking. This research comprises of the following steps

1. Neighbour discovery
2. Gateway selection
3. Security
4. Broadcasting

Primarily, the table generated for storing the neighbours information. The topology is generated for the total no. of vehicles in the network. The sensors in the vehicles used to capture the traffic details and location of the node. An optimal wireless Access in VANET (OWAV) Protocol based on IEEE 802.11p is used to reduce the delay and latency of the vehicular network. For secure communication, Dual Encryption technique is used. For secure broadcasting of

messages, the WAVE protocol [11] is incorporated with optimal encryption algorithms.

Neighbour Discovery

A table generated for effective communication for the vehicles available in the network which contains the neighbouring node's information, topology data etc. The IEEE 802.11p based Optimal Wireless Access in VANET (OWAV) Protocol is utilized for this process. The main intension is to enhance the reliability and minimize the latency during communication. OWAV aims to maintain interoperability and tough protected infrastructure in a vehicular environment. This protocol is the multi-hop broadcasting mechanism which is suitable for multichannel transmission of infotainment data. This research ensures reliable data transmission with less delay.

Gateway selection

Based on the communication range the gateways (static) are positioned at road side. The present location is updated on gateway by each and every vehicles. The election of suitable gateway is based on auto configuration, because it operates as a location server and accumulates the data about position of the vehicles. After the selection of optimal gateway, all the vehicles in the network are registered with distinctive username and password. Then it remits the registration request to Highway influence through a protected medium. A random unique number is created for processing the identification of the demanded vehicle after receiving the request.

Secured Data Dissemination using optimal blow fish algorithm

Here we are using optimal encryption algorithm for secure transmission. The security problem is also a major issue in this research, while transmitting the data among various vehicles during emergency message broadcasting. Exposing high confidential information or data such as medical report, military or defence information to unauthorized person causes heavy damages. To evade these issues, compulsory secured data dissemination mechanism is needed.

- The proposed security mechanism prevents broadcast storm issue.
- It is extremely sufficient and has intension to deal with dense and narrow density networks.

Here we propose an optimal encryption technique for securing vehicle related information to avoid unauthorized access. The Blow fish algorithm based on oppositional deer hunting algorithm (ODHO) is used to securely transmit the emergency messages over vehicular network. The key generation process is optimally done using ODHO algorithm.

Optimal Blow Fish Algorithm

A symmetric key cryptography based blow fish algorithm is used along with optimization algorithm for enhanced security. It includes 64 bit block size and key size from 32 bit to 448 bits. There is P-array and four 32 bit S-boxes. P-array comprises 18 of 32 bit sub keys and each S-box contains 256 entries. It comprised of 2 phases such as expansion of key and encryption process. In key expansion, the input keys are divided into sub keys. Sixteen round feistel network is exploited for encryption process in which permutation and key updation will be done in each round. This key generation process can be done by Oppositional deer hunting algorithm. The optimal key with maximum key breaking time will be used for encryption process.

Key generation process

Enormous no. of secondary keys is applied in this encryption process. These secondary keys must be precompiled prior to the cryptographic process.

- P-array contains 18 of 32 bit sub keys ie., $P_{y1}, P_{y2}, ,, \ldots P_{y18}$
- four 32 bit S-box contains 256 entries

$$S_{b1,0}, S_{b1,1}, \cdots, S_{b1,255}$$
$$S_{b2,0}, S_{b2,1}, \cdots, S_{b2,255}$$
$$S_{b3,0}, S_{b3,1}, \cdots, S_{b3,255}$$
$$S_{b4,0}, S_{b4,1}, \cdots, S_{b4,255}$$

Encryption

Conversion of original data into another form is known as encryption. The size of input data is 64 bits which is divided in to two 32 bit part in the initial round and described as LH and RH part. The XOR operation done for LH part and p array and the results is stored in function F_t. The results and the next part RH are carried the next XOR operation. Finally the results and interchanged until 16 round completes. It is presented in Fig. 1.

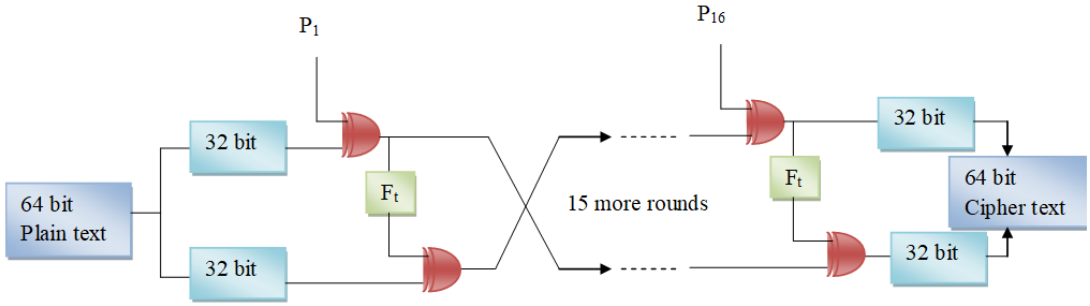

Fig.1. Encryption process of Blowfish algorithm

Principle of Ft function

This function comprises of four S-boxes with size 32 bit which includes 256 entries. This 32 bit divided into 4 blocks with size 8 bit each and represented by m, n, o, and p respectively. The Principle of this function is described in fig. 2.

$$F_t(L_H) = ((S_{b1,m} + S_{b2,n} \bmod 2^{32}) \oplus S_{b3,0}) + S_{b4,p} \bmod 2^{32} \quad (1)$$

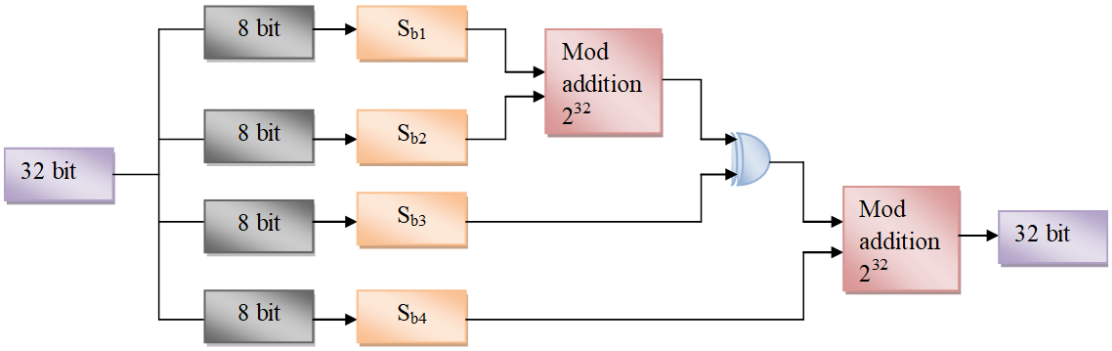

Fig.2. Principle of Ft functions

Decryption

The reverse process of P-Array is performed on the decryption process of blow fish algorithm.

Oppositional Deer Hunting Optimization (ODHO)

Here, in this research, optimal key will be generated for encryption to ensure the security. ODHO algorithm is used to optimal key generation process in blowfish algorithm. In ODHO, the main intention of the proposed algorithm is to identify the optimal location for the man to search the deer, it is essential to know the characteristics of the deer [18]. Their unique behaviour makes predators a huge difficulty in hunting. Deer's had high and sharp visuality which is 5 times better than humans. But they won't differentiate green and red colors. One of the variety of deer ie, white tailed deer has 250-270 degree peripheral vision in which can able to identify a small move. This type of deer is also known as buck. This peripheral vision of a deer assists to locate the position of the hunter within the range. The hunter is allegedly moved to the top of the tree means the deer can't able to sense the movement which is out of the range.

The deer can stink 60% more than the man which its olfactory sensors. It can smell sixty times better than humans with its olfactory sensors. If the deer identifies the danger means it treading heavily and sniffing loudly to alert other deer's. But the hearing ability of deer is poor than the man which ranges from 3000-8000 hertz only. But it can hear UHF sounds which is not possible by humans. The ears of deer are roll around to sense different sounds which is similar to satellite chips.

Algorithm

Initialization

Let N be the total number of hunters in which they represents the solution of the population Q

$$Q = \{Q_1, Q_2, \cdots, Q_N\} \quad (2)$$

Nearest mediate opposition behaviour learning (NMOBL)

Tizhoosh presented an intellectual method to improve the search speed known as Opposition based Learning (OBL) [19]. In this method, both the solution and the reverse solution are used for searching operation. The Opposition solution can be estimated using the minimum and maximum boundary constraints. In our method, the OBL is further enhanced as Nearest Mediate OBL (NMOBL). Here the opposition solution is estimated using nearest mediate points. More than one center of gravity or mediate points are used to maintain the diversity of the group. Like in PSO, tiny groups of various parts can search multiple areas in solution space. In reverse calculation, multiple center of gravity points are used to perform search operation with a help of small search groups. The major advantage of our NMOBL is the Opposite solution can search more search space with the help of multiple center of gravity points. It will help to converge the solution fast.

Definition

The center of gravity for the population Q defined in eqn.

$$M_j = \frac{\sum_{j=1}^{D} Q_{ij}}{N} \text{ where, i=1,2,...,N} \tag{3}$$

Here D represents the entire search space and M represents the center of mass of discrete uniform, then the reverse solution point of Q_i, is described as

$$\overrightarrow{Q_i} = 2 \times M - Q_i \text{, where i=1,2,...N} \tag{4}$$

The reverse points are placed in the solution space with adaptive boundary constraints which is $Q_{ij} \in [aj,bj]$. These boundaries can permit the reverse points to be placed in a reducing solution space.

$$a_j = \min(Q_{ij}) \tag{5}$$

$$b_j = \max(Q_{ij}) \tag{6}$$

If the reverse point surpasses the boundary it is updated using the following equation

$$\vec{Q}_{i,j} = \begin{cases} a_j + rand(0,1) \times (M_j - a_j), & if \quad \vec{Q}_{i,j} < a_j \\ M_j + rand(0,1) \times (b_j - M_j), & if \quad \vec{Q}_{i,j} > b_j \end{cases} \tag{7}$$

The nearest mediate opposition point is

$$Q_i^* = 2 \times k \times M_i - Q_i$$

Where M_i is the number of agents in the nearest position and a random number k is used.

Parameter initialization

Let be initialize the important variables such as position of deer and wind angle to identify the location of hunters. If the solution space is a circular path, the circumference of the path is presented by wind angle

$$\theta_i = 2\pi \, rand \tag{8}$$

rand represents the random number and i stands for iteration and deer's angle position is given by

$$\phi_i = \theta + \pi \tag{9}$$

Here wind angle is represented by θ

Propagation of Position

The Optimal position in the search space is unknown and it is assumed initially. It is determined based on the

fitness function. In this method, leaders position Q^{Ldr} and position of the successor Q^{Sucr} are considered as the solution.

Leader position updation

Every individual in the initial population try to achieve the finest solution by updating the position. The circular behaviour id described as

$$Q_{i+1} = Q^{Ldr} - P.\ x.\ \left| L \times Q^{Ldr} - Q_i \right| \tag{10}$$

Here the position of current iteration and next iteration are presented as Q_i and Q_{i+1} respectively. The wind speed is presented by x which is a random number ranges from zero to two. The coefficient vectors are P and L.

$$P = \frac{1}{4}\log\left(i + \frac{1}{i_{\max}} \right)\beta \tag{11}$$

$$L = 2.\gamma \tag{12}$$

Here maximum iteration is described by i_{max}. Random numbers β and γ ranges -1 and 1 and 0 to 1 respectively. The initial position (Q,R) is updated based on the location of prey ie., deer. The location of agent is moved if the optimal position (Q*,R*) is attained by using P and L. Every hunter in the initial solution travels towards the leader position if the movement is successful. The position updation process is explained in Fig. 3.

Position angle updation

The angle updation is necessary for identifying the hunter position if the prey doesn't know about the attack. It is described as

$$\alpha_i = \frac{\pi}{8} \times rand \tag{13}$$

the angle position is updated using the difference among wind angle and visual angle of the deer

$$d_i = \theta_i - \alpha_i \tag{14}$$

$$\phi_{i+1} = \phi_i + d_i \tag{15}$$

$$Q_{i+1} = Q^{Ldr} - x\ .\ \left| \cos(\nu) \times Q^{Ldr} - Q_i \right| \tag{16}$$

Where Q_i^* indicates the optimal position. Here the location of the individual is opposite to the position angle in order that the hunter is not in the vision of deer.

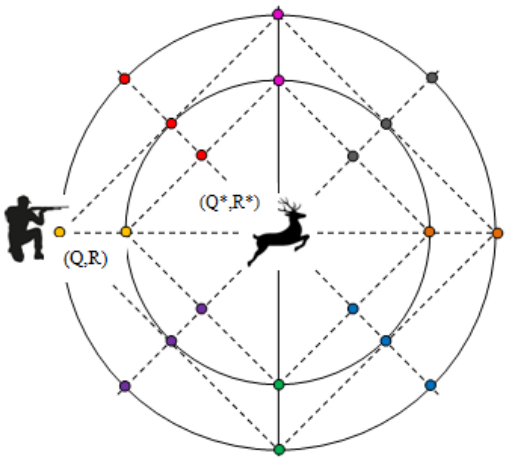

Fig.3. Position updation process of ODHO

Successor position updation

In the searching phase, the similar process in encircling behaviour can be assumed by fine-tuning the vector L. Initially the vector L is considered as <1 as random. Consequently, the updation of the finest position is estimated using the successor position which allows global search. This allows a global search as represented by the following

$$Q_{i+1} = Q^{sucr} - P.\ x\ .\ \left| L \times Q^{sucr} - Q_i \right| \tag{17}$$

Q^{sucr} describes the next position of the search agent or hunter in current population

Based on the solution obtained the position of agents are updated at each iteration to get the optimal solution. Moreover, the parameters required to be adjusted are only two, i.e. P and L, which adds to the benefit of the algorithm.

Termination

The process is repeated until the best solution is obtained and the process is terminated based on objective function.

Table 1. Pseudo code for ODHO

```
Input : Initialized Population Q
Output: First optimal solution Q^Ldr and 2nd optimal solution Q^Sucr
Begin
    while (i<i_max)
        For each solution in the population
            Compute the fitness of each solution
            Update α, β, γ, L, P, d and x
            If (P<1)
                If(|L|>=1)
                    Update the position of the individual
                Else
                    Update the position of the individual
                End if
            Else
                Update the position of the individual
            End if
        End for
    Compute the fitness of each solution
    Update Q^Ldr and Q^Sucr
    Calculate the neighbourhood centroid M'
    Calculate opposite position OQ
    Update dynamic interval boundaries
    Check the boundary constraint violations
    Calculate the fitness of opposite position
     For i=1 to N do
        if f(OQ_i<f(Q_i) then
            Q_i=OQ_i
        end if
     end for
        i=i+1
     End while
     Return Q^Lead
Terminate
```

Broadcasting

The emergency data, climate or weather conditions, traffic information are shared in VANET during broadcasting process. Various issues such as broadcast storm, network terminal problem etc are occur based on huge number of concurrent communications. The location and position of the sending vehicle is changed due to high mobility so, it is necessary to choose the destination to share the message. The secured transmission efficiently improves the speed of broadcasting. The major highlights are, 1) Improved security 2) Enhanced efficiency on communication 3) Minimized latency and delay.

4. Results and Discussion

The proposed research is implemented in Network Simulator (NS2). The proposed research is examined for both highway and urban scenarios. The alert during emergency situation is disseminated to vehicles by the Road Side Unit in high ways which is originated commonly at regular intervals. While transferring the information among vehicles, malicious vehicle, attackers, unauthorized persons may try to extract the emergency data. Here we have analyzed various types of attacks such as brute force, DOS and Sybil etc.

Performance Metrics

Packet delivery ratio (PDR) is described as the ratio among total no. of broadcasted packets and received packets

$$PDR = \frac{No.of\ successfully\ received\ packets}{No.of\ tranmitted\ packets} * 100 \tag{18}$$

Transmission Delay is the instance occupied by the data packet to move from source to destination via communication medium. Its unit is millisecond.

Routing control overhead defined as the proportion of the control information which was completely sent to the data that was really received by the node in the network. It is estimated based on the functions of link maintenance, latency, and node discovery.

Throughput is the avg. rate of successful message delivery at destination via transmission medium

Key computation time is described as the time occupied to estimate the key for authentication. Similarly, the time taken to re-compute the key is known as **key recovery time**. It is estimated with various sizes

Comparative Analysis:

Here table 2 represents encryption time analysis of different algorithms ie, the time taken to encrypt the data with different lengths. Our proposed encryption algorithm outperforms the existing algorithms with less encryption time.

Table 2. Analysis of encryption time

Algorithms	Encryption time(inms)
AES	336
RSA	345
ECC	284
Proposed encryption method	265

In this research, the proposed encryption algorithm encodes the emergency data in less duration. The efficiency of the encryption algorithm, different attacks such as DOS, Brute force attack, MiM and Sybil attack are analyzed in Table 3.

Table 3. Key similarity analysis

Algorithm	Similarity (in %)			
	DOS attack	Sybil attack	Brute Force Attack	MIM attack
AES	25.58	23.44	23.16	25.18
RSA	22.54	21.65	21.34	22.84
ECC	19.35	18.46	19.98	19.65
Proposed encryption method	12.21	13.32	13.43	14.06

The resemblance among the hacked data and the original data is analyzed using a distance measure. Our proposed encryption technique outperforms other methods because of optimal key generation process. The key breaking time is high for the proposed method because it strongly fighting with malicious nodes and unauthorized nodes to ensure security. Here the key breaking time is high for our proposed optimization algorithm whereas the others perform less. This key breaking time is used for fitness in Oppositional deer hunting algorithm. It is given in fig. 4.The other algorithms such as WOA, DHO, GWO are used for optimal key generation process which will obtain less key breaking time as fitness. Because of oppositional behaviour in ODHO, it selects finest prime number as key for encryption so that the key breaking time is high for the proposed algorithm.

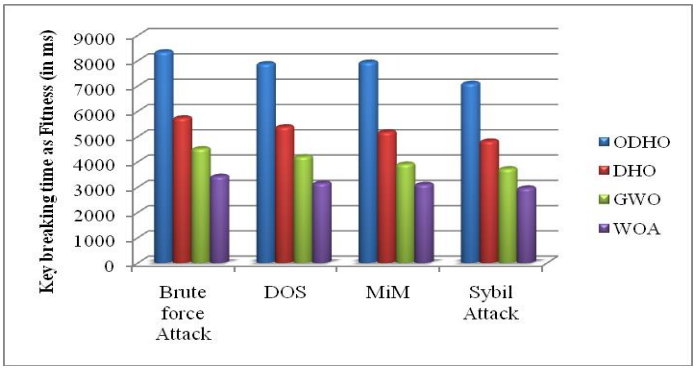

Fig.4. Comparative analysis on key breaking time

Here in ODHO algorithm, the key breaking time is used as the fitness for the ODHO algorithm, ie., how much time it will take to break the key when an unauthorized vehicle hacks the message. The objective of this problem is maximization, so the fitness value converges nearer to maximum time. Our ODHO algorithm has maximum fitness when compared to others. The ODHO is a global search algorithm which has fastest convergence.

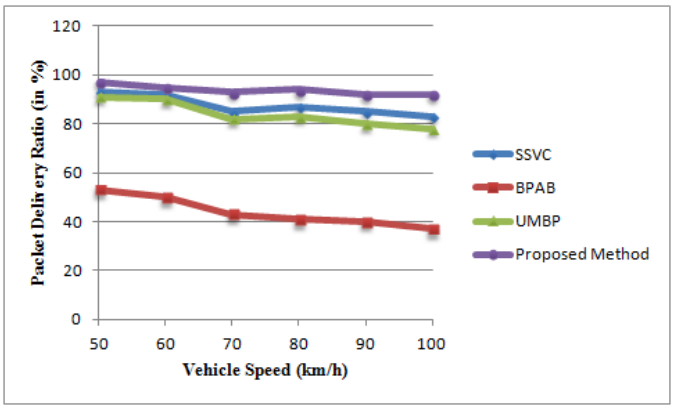

Fig.5. PDR in varying vehicle speed

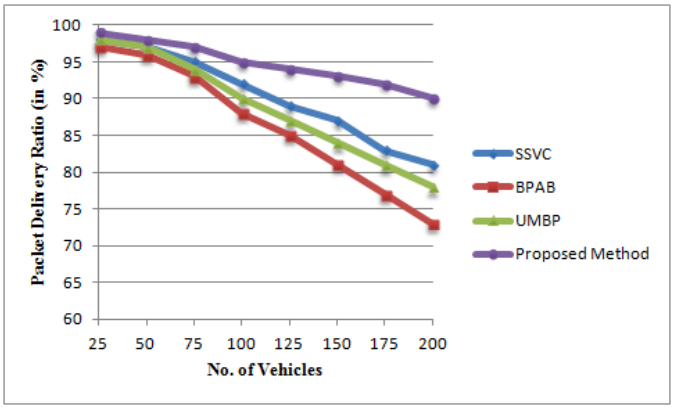

Fig.6. PDR in varying network densities

PDR with various vehicle density and speed can be analyzed in Fig. 5 and 6. Our proposed research concentrates on reliable and secure transmission of emergency messages so it yields high PDR value when compared to the other methods. The encryption algorithm securely broadcast the emergency messages and the encryption algorithms prevents the messages from unauthorized vehicles.

At a density of 25-50 vehicles, we observed nearly 99% of successful transmissions for the Proposed method against existing methods such as SSVC [20], BPAB, UMBP [21] etc; When the vehicle density increases, the PDR value drops gradually for the existing methods but it remains stable for the proposed scheme.

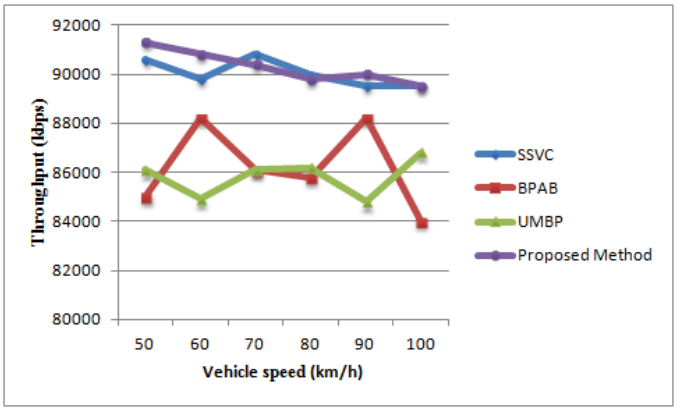

Fig.7. Analysis on Throughput

Fig. 7 shows the analysis of throughput withrespect to the vehicle speed (km/h). It is observed that the througput is increasing with incresing vehicle speed which is better when evaluated with other techniques. The throughput of the existing protocols is low because of malicious attacks. The optimal encryption technique increases the throughput of the proposed research.

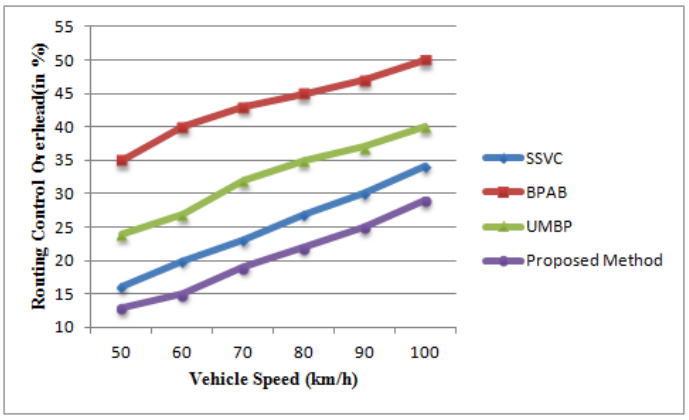

Fig.8. Analysis on Routing Control Overhead with varying vehicle speed

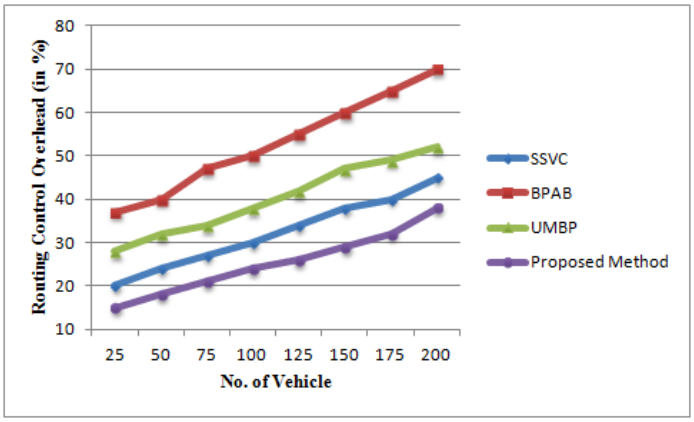

Fig.9. Analysis on Routing Control Overhead with varying vehicle density

Fig. 8 and Fig. 9 analyzes the routing overhead measure with varying vehicle density and speed. With the optimal gateway selection process, our proposed method has reduced routing overhead. The other techniques having high values when the no.of vehicles and vehicle speed increases.

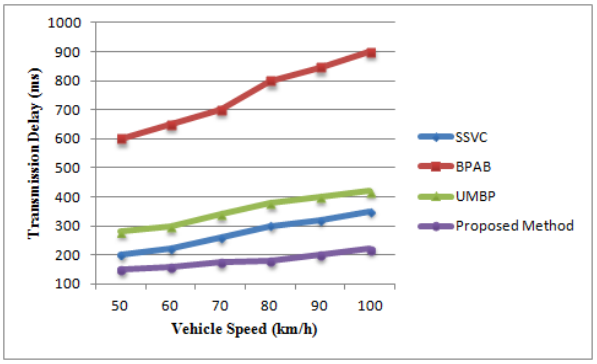

Fig.10. Analysis on Transmission delay

Delay in emergency message broadcasting leads severe damage in road safety and traffic. The proposed optimal and secured transmission technique provides less delay in data transmission when compared to the other methods as described in Fig. 12. When the vehicle speed increases the proposed method transmission delay also increases.

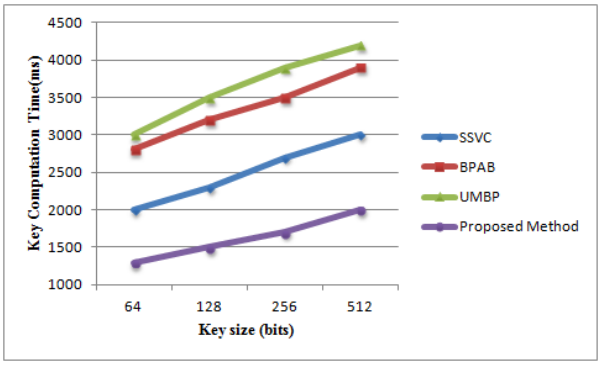

Fig.11. Key computation time analysis

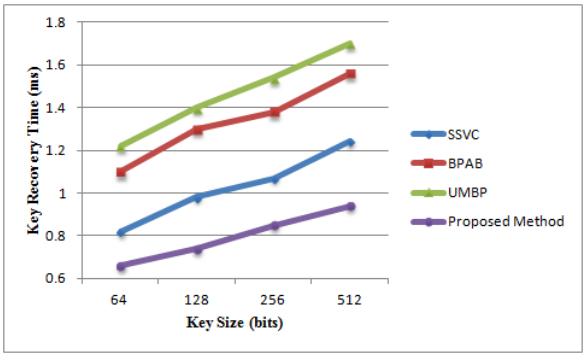

Fig.12. Key Recovery Time analysis

While using cryptographic algorithms, the efficiency is estimated in terms of key computation time, key recovery time, key breaking time etc. It is presented in Fig. 11 and Fig. 12. When compared to other techniques such as SSVC, BPAB our proposed method took less time to generate the optimal keys for both encryption and decryption process because of effective optimization algorithm.

From the results and analysis part, the proposed method broadcast the emergency messages with high security and reliability.

5. Conclusion

Emergency Message broadcasting is a important process in VANET. Security and reliable transmission are the two major concerns in VANET message broadcasting. The maintenance of security is a major problem of VANET, here the message broadcasting is affected due to no.of constraints such as malicious nodes, attacks, un-authorization, eavesdropping, MiM etc. The primary objective of this research is to reduce latency and provide high reliable and efficient communication over the vehicles. Primarily, the data such as vehicle position, location, speed, and other traffic information's are generated and stored in a separate table. To ensure the secured transmission, a specific connection is

established for tracking the vehicle information. Blowfish encryption algorithm along with Oppositional deer hunting optimization (ODHO) is used to store the trusted vehicles location to avoid unauthorized tracking. The key generation process is done using optimization so that the hackers not able to break the key easily. The convergence of optimization algorithm is based on maximum key breaking time. The encryption analysis is done with varying key size (in bits). From the comparative evaluation, it is observed that the proposed method outperforms other techniques by efficiently storing the vehicle information in a secured location using optimal Blowfish algorithm. The performance is analyzed with different attacks and with varying vehicle density and vehicle speed.

This research is further extended in future with hybrid and modified encryption technique which will give enhanced security to the emergency message broadcasting system. Then improvement in the encryption setup gives high security over passive and active attacks.

References

[1] Muhammad Awais Javed, Duy Trong Ngo and Jamil Yusuf Khan, "A multi-hop broadcast protocol design for emergency warning notification in highway VANETs." *EURASIP Journal on Wireless Communications and Networking* 179(2014):pp. 1-15.

[2] Manivannan, Shafika Showkat Moni, Sherali Zeadally,"Secure authentication and privacy-preserving techniques in Vehicular Ad-hoc NETworks (VANETs)." *Vehicular Communications* 25(2020):pp.1-18.

[3] Salim Bitam, Abdelhamid Mellouk, Sherali Zeadally, "VANET-cloud: generic cloud computing model for vehicular Ad Hoc networks." *IEEE Wirel. Commun* 22 (2015): pp. 96–102.

[4] Mohamed Nidhal Mejri,Jalel Ben-Othman, Mohamed Hamdi, "Survey on VANET security challenges and possible cryptographic solutions." *Veh. Commun.* 1.2 (2014):pp. 53–66.

[5] Wenshuang Liang, Zhuorong Li, Hongyang Zhang, Shenling Wang, Rongfang Bie , "Vehicular ad hoc networks: architectures, research issues, methodologies, challenges, and trends." *Int. J. Distrib. Sens. Netw*. 11.8 (2015):pp. 1-11.

[6] Vaibhav, Dilendra Shukla, Sanjoy Das, Subrata Sahana, "Security challenges, authentication, application and trust models for vehicular ad hoc network—a survey." *Int. J. Wirel. Microw. Technol*. 3 (2017):pp. 36–48.

[7] Fengzhong Qu, Zhihui Wu, Fei-Yue Wang, Woong Cho, "A security and privacy review of VANETs." *IEEE Trans. Intell. Transp. Syst.* 16 (2015):pp.2985–2996.

[8] Bingyi Liu, Dongyao Jia Jianping Wang, Kejie Lu, Libing Wu, "Cloud-assisted safety message dissemination in VANET—cellular heterogeneous wireless network." *IEEE Syst. J.* 11.1 (2017):pp.128-139.

[9] Richard Gilles Engoulou, Martine Bellaïche,Samuel Pierre, Alejandro Quintero, "VANET security surveys." *Comput. Commun.* 44 (2014):pp.1–13.

[10] R. Raiya, S. Gandhi, Survey of various security techniques in VANET, Int. J. Adv. Res. Comput. Sci. Softw. Eng. 4 (2014).

[11] Y. L. Morgan, "Managing DSRC and WAVE standards operations in a V2V scenario." *International Journal of Vehicular Technology* (2010):pp.1-18.

[12] Tzeng, Shiang-Feng, et al, "Enhancing security and privacy for identity-based batch verification scheme in VANETs." *IEEE Transactions on Vehicular Technology* 66.4 (2017): pp.3235-3248.

[13] Tangade, S. Manvi S. S and Lorenz, P, "Decentralized and Scalable Privacy-Preserving Authentication Scheme in VANETs." *IEEE Transactions on Vehicular Technology*, (2018): pp.1-10.

[14] Muthumeenakshi, R., T. R. Reshmi, and K. Murugan, "Extended 3PAKE authentication scheme for value-added services in VANETs." *Computers & Electrical Engineering* l. 59 (2017): pp. 27-38.

[15] Dressler, F., Klingler, F., Sommer C., and Cohen, R, "Not All VANET Broadcasts Are the Same: Context-Aware Class Based Broadcast." *IEEE/ACM Transactions on Networking* 26.1 (2018): pp. 17-30.

[16] Feukeu, E.A., Zuva, T, "Dynamic Broadcast Storm Mitigation Approach for VANETs." *Future Generation Computer Systems* (2014):pp.1-8.

[17] Daxin Tian,Chao Liu, Xuting Duan, Zhengguo Sheng, Qiang Ni,Min Chen,and Victor C.M. Leung, "A Distributed Position-Based Protocol for Emergency Messages Broadcasting in Vehicular Ad Hoc Networks." *IEEE Internet of Things Journal* 5.2 (2014):pp. 1218-1227.

[18] Brammya, G, Praveena, S., Ninu Preetha, N.S., Ramya, R., Rajakumar B.R., and Binu, D, "Deer Hunting Optimization Algorithm: A New Nature-Inspired Meta-heuristic Paradigm" *The Computer Journal* (2018):pp.1-20.

[19] Mirjalili S, Mirjalili SM, Lewis A., "Grey Wolf Optimizer." *Advances in Engineering Software* 69.3 (2014): pp. 46-61.

[20] Sathya Narayanan P.S.V, "A sensor enabled secure vehicular communication for emergency message dissemination using cloud services." *Digital Signal Processing* 85 (2019): pp. 10-16.

[21] Yuanguo Bi, Hangguan Shan, Xuemin Sherman Shen, Ning Wang, Hai Zhao, "A Multi-Hop Broadcast Protocol for Emergency Message Dissemination in Urban Vehicular Ad Hoc Networks." *IEEE Transactions on Intelligent Transportation Systems* 17.3 (2016).

[22] S. Zeadally, R. Hunt, Y.-S. Chen, A. Irwin, and A. Hassan, "Vehicular ad hoc networks (VANETS): status, results, and challenges." *Telecommunication Systems* 50.4 (2012):pp. 217–241.

[23] F. Qu, Z. Wu, F. Wang, and W. Cho, "A security and privacy review of VANETs." *IEEE Transactions on Intelligent Transportation Systems* 16.6 (2015):pp. 2985–2996.

[24] R. Mishra, A. Singh, and R. Kumar, "VANET security: issues, challenges and solutions." *in Proceedings of the International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT)*, pp. 1050–1055, Chennai, India, March 2016.

[25] J. Cui, L. Wei, J. Zhang, Y. Xu, and H. Zhong, "An efficient message-authentication scheme based on edge computing for vehicular ad hoc networks." *IEEE Transactions on Intelligent Transportation Systems* 20.5 (2019):pp. 1621–1632.

[26] R. Akalu, "Privacy, consent and vehicular ad hoc networks (VANETs)." *Computer Law & Security Review* 34.1 (2018): pp. 37–46.

[27] K. Bylykbashi, D. Elmazi, K. Matsuo, M. Ikeda, and L. Barolli, “Effect of security and trustworthiness for a fuzzy cluster management system in VANETs.” *Cognitive Systems Research* l. 55, pp. 153–163, 2019.
[28] J. P. Hubaux, S. Capkun, and J. Jun Luo, “The security and privacy of smart vehicles.” *IEEE Security & Privacy Magazine* 2.3(2004):pp. 49–55.
[29] M. Azees, L. Jegatha Deborah, and P. Vijayakumar, “Comprehensive survey on security services in vehicular adhoc networks.” *IET Intelligent Transport Systems* 10.6 (2016):pp. 379–388.
[30] Sivaraj C, Alphonse P J A, Janakiraman T N,"Energy-efficient and Load Distributed Clustering Algorithm for Dense Wireless Sensor Networks", International Journal of Intelligent Systems and Applications(IJISA), Vol.9, No.5, pp.34-42, 2017. DOI: 10.5815/ijisa.2017.05.05
[31] Hamdy M. Mousa, "Bat-Genetic Encryption Technique", International Journal of Intelligent Systems and Applications(IJISA), Vol.11, No.11, pp.1-15, 2019. DOI: 10.5815/ijisa.2019.11.01
[32] Krishna S.R.M., Seeta Ramanath M.N., Kamakshi Prasad V.,"Optimal Reliable Routing Path Selection in MANET through Novel Approach in GA", International Journal of Intelligent Systems and Applications(IJISA), Vol.9, No.2, pp.35-41, 2017. DOI: 10.5815/ijisa.2017.02.05

Authors’ Profiles

Mrs. M. Selvi received her B.Sc Computer Science degree from S. T. Hindu college affiliated Manonmaniam Sundaranar University, Tirunelveli, India and MCA degree from Anna University, India. She has completed the M.phil degree in Computer Science in Manonmaniam Sundaranar University. Presently she is a research scholar in Department of Computer Science, S. T. Hindu College, Nagercoil affiliated to Manonmaniam Sundaranar university, Tirunelveli. She has six years of research experience and authored more than ten research papers in SCI and Scopus indexing journals. His research interests include Data Mining, Information Security, Vehicular Network and Network Security.

Dr. B. Ramakrishnan is currently working as Associate Professor in the Department of Computer Science and research Centre in S.T. Hindu College, Nagercoil. He received his M.Sc degree from Madurai Kamaraj University, Madurai and received Mphil (Comp. Sc.) from Alagappa University Karaikudi. He earned his Doctorate degree in the field of Computer Science from Manonmaniam Sundaranar University, Tirunelveli. He has a teaching experience of 30 years. He has 23 years of research experience and published more than 50 research articles in reputed international journals (12 Science Citation Index Expanded research articles at Springer Journals and 22 SCOPUS indexed research articles). Further, he has authored a book titled “Vehicular Ad Hoc Network and Web Vehicular Ad Hoc Network an Overview” published by the International book publisher LAP Lambert Academic Publishing with the ISBN:978-3-330-02628-5. His research interests lie in the field of Vehicular networks, mobile network and communication, Cloud computing, Green computing, Ad-hoc networks and Network security.

How to cite this paper: M. Selvi, B. Ramakrishnan, "Secured Message Broadcasting in VANET using Blowfish Algorithm with Oppositional Deer Hunting Optimization", International Journal of Computer Network and Information Security(IJCNIS), Vol.13, No.2, pp.39-52, 2021. DOI: 10.5815/ijcnis.2021.02.04