Wireless Networks (2020) 26:4207–4226
https://doi.org/10.1007/s11276-020-02325-z

Vehicular networks with security and trust management solutions: proposed secured message exchange via blockchain technology

Nisha Malik[1] · Priyadarsi Nanda[1] · Xiangjian He[1] · Ren Ping Liu[1]

Published online: 20 April 2020

Abstract

In vehicular ad hoc networks (VANET), effective trust establishment with authentication is an important requirement. Trust management among communicating vehicles is significant for secure message transmission; however, very less contributions have been made towards evaluating the trustworthiness of the node. This research work intends to introduce a new trust management system in VANET with two major phases: secured message transmission and node trustability prediction. The security assured message passing is carried out by incorporating the privacy preservation model under the data sanitization process. The key used for the sanitization process is optimally tuned by a new hybrid algorithm termed Sea Lion Explored-Whale Optimization Algorithm, which is the combination of Whale Optimization Algorithm and Sea Lion Optimization Algorithm, respectively. The blockchain technology is assisted to handle the key generated by the nodes. Subsequently, the trustability of the node is evaluated under novel specifics "two-level evaluation process" with a rule-based and machine learning-based evaluation process. Finally, the performance of the proposed model is verified and proved over other conventional methods for certain measures.

Keywords VANET · Trust evaluation · Data sanitization · Key generation · Optimization

Abbreviations

5G	Fifth generation
CRL	Certificate revocation list
RSU	Roadside unit
QoS	Quality-of-service
P2P	Peer-to-peer
BARS	Blockchain-based anonymous reputation system
JSSDT	Joint spectrum sensing and data transmission
IGHSOM	Improved growing hierarchical self-organizing map
CL-PKS	Certificateless public key signature
V2I	Vehicle-to-infrastructure
HTM	Hybrid trust model
MDS	Misbehavior detection system
PoW	Proof of work
MN	Mobile node
OBU	On board units
KCA	Known ciphertext attack
CPA	Chosen plaintext attack
CCA	Chosen ciphertext attack
SOM	Self organizing map
KPA	Known plaintext attack
GHSOM	Growing hierarchical self-organizing map
PDR	Packet delivery rate
PFR	Partnerships for renewables
RSSI	Recieved signal strength indicator
VANET	Vehicular ad hoc networks
CR-VANET	Cognitive radio VANET
IDS	Intrusion detection system
V2V	Vehicle to vehicle
WOA	Whale Optimization Algorithm
MCC	Mobile cloud computing
NPV	Net present value

✉ Nisha Malik
mnishamalik39@gmail.com

Priyadarsi Nanda
nandapriyadarsi9@gmail.com

Xiangjian He
xiangjianhe887@gmail.com

Ren Ping Liu
RenPing.Liu@uts.edu.au

[1] Faculty of Engineering and IT, University of Technology Sydney, Sydney 2007, Australia

1 Introduction

Autonomous vehicles in VANET-the spontaneous creation of a wireless network for data exchange to the domain of vehicles may pave the way for future systems where computers take over the art of driving. It aids in transferring secure messages for proper communication between the vehicles. The entire infrastructures and smart vehicles comprise the vehicular network and that has emerged as a noteworthy scenario in the 5G mobile networks [1–4]. The road-related messages are shared with their neighbors by vehicles using the Vehicular networks [5–7], for instance: traffic congestions, road conditions, and so on. This in turns offers the vehicle about the traffic situations and thereby enhances transportation efficiency and safety. Even though, the neighboring vehicles are not completely trusted due to the large variability and mobility of vehicular networks. This is considered as a serious issue at the time of the existence of more malicious vehicles within the network. Some of these issues are the capability of the network to self-organize within a high mobile network environment, the trustworthiness evaluation of nodes participating in VANETS [8–13] and their misbehavior detection, the revocation process and the CRL management and distribution.

Trust management scheme facilitates the vehicles to decide on the trustworthiness [14–16] of the received message, and as well offers the network operators the basis of punishments or rewards on appropriate vehicles. Generally, a particular vehicle's trust value is evaluated based on its past behavior's ratings produced by pertinent nodes. Existing trust management systems can be classified into two groups, i.e., centralized and decentralized [13]. In the centralized trust management schemes, the entire ratings are processed and stored within a central server, for instance: cloud server. The decision making is made by the vehicles in a fairly short delay. Due to this, the centralized schemes will not always please the meticulous QoS [17, 18] needs in vehicular networks. In the decentralized trust management schemes, the occurrence of trust management tasks is made within the vehicle or in the RSU. The interactions with network infrastructures are reduced because of the local management of trust values. Data sanitization policies, procedures and requirements are mentioned in many data protection and privacy regulations and guidelines. The optimization concept [19–21] plays a major role in making the sanitization more promising.

Recently, blockchain technology plays its major role in many of the applications particularly in VANET, since it can solve more critical problems of information dissemination in VANETs. Moreover, the technology is considered as the distributed and decentralized computing paradigm that underpins the Bitcoin cryptocurrency that grants both security and privacy in P2P networks. In VANET, the blockchain is used to maintain the ground truth of information for vehicles as any vehicle could access event information' history in the public blockchain [22].

Research Objectives and contribution:

- This work presents a new trust management system in VANET using two major stages named Secured Message Transmission and Node Trustability Prediction.
- The assurance of secured message transmission via blockchain technology is given by integrating the privacy preservation model under the Data Sanitization process.
- The key used for the sanitization process is tuned optimally using a new hybrid algorithm named SLE-WOA, which combines the theory of WOA and SLnO algorithm, respectively.
- After this, the node trustability is computed in terms of novel terms "two-level evaluation process" via rule based and machine learning-based evaluation process.
- To the end, the performance of the implemented model is validated over other state-of-the-art methods for certain measures.

This paper is organized as follows: Sect. 2 defines the literature survey on the contributed papers regarding VANET. Section 3 describes the VANET simulation and proposed the trustability prediction and data hiding process. Section 4 explains the procedure of optimal key by a hybrid algorithm that combines the SLnO and WOA models. Section 5 defines the results and their discussions. Section 6 terminates the paper.

2 Literature survey

2.1 Related works

In 2019, Shrestha et al. [22] have proposed a novel blockchain model to determine the crucial message dissemination problems in VANET. Further, a local blockchain for real-world event message exchange was created amongst the vehicles in the boundary of a country. This was assumed as a novel kind of blockchain appropriate for VANET. Subsequently, a public blockchain was presented that stores the message trustworthiness and node trustworthiness within a distributed ledger for secure message dissemination. It requires plenty of computing power. Most of the malicious miners could capture the network and gain dominance, thereby making decentralization a failure.

In 2019, Yang et al. [13] have introduced a decentralized trust management scheme based on blockchain approaches in vehicular networks. Moreover, the Bayesian Inference method was used by vehicles for validating the

received messages from neighboring vehicles. A rating was generated by the vehicle for every message source vehicle based on justification outcome. Further, the trust value offsets of comprised vehicles were computed using RSUs depending on ratings uploaded from vehicles, and packed these data within a "block". Subsequently, every RSU tries to add their "blocks" to the trust blockchain. The experimental analysis has revealed that the implemented structure was feasible and effective in calculating, storing and collecting trust values in vehicular networks. It can produce posterior distributions that are heavily influenced by the priors. It often comes with a high computational cost, especially in models with a large number of parameters.

In 2018, Liu et al. [23] have implemented BARS for establishing a privacy-preserving trust technique for VANETs. The implementation of the certificate and revocation transparency was made based on the expanded blockchain technology. Further, for avoiding the forged message distribution, a new algorithm named reputation evaluation was introduced that relies on indirect opinions about vehicles and direct historical interactions. Later, the BARS evaluation was performed using a set of experiments regarding the validity, security, and performance, and the outcomes have shown the better establishment of the trust model with conditional anonymity, transparency, robustness and efficiency for VANETs. The most important limitation of BARS is time-consuming, difficult, and also it is expensive.

In 2019, He et al. [24] has presented a general work to learn about trust management for improving the data transmission and spectrum sensing processes in CR-VANETs. Further, a novel JSSDT attack has been proposed in the data transmission process, where an attacker could be reported for fake sensing data and packet drops. Afterward, a unified trust management structure was proposed in CRVANETs for both processes. Based on this scheme, a weighted consensus-based spectrum sensing structure was introduced for preventing the spectrum sensing process. The analysis thus implied the efficiency of the introduced trust-based security structures. Weight selection is a crucial step in this method, because the entire performance relies on the weights included in the spectrum sensing model. Inappropriate weights may lead to uncertainty in the performance achievement.

In 2019, Liang et al. [25] have established new IDS for wireless and dynamic networks, such as VANETs. The IDS was mainly incorporated with a new algorithm including feature extraction and classifier based on IGHSOM in VANETs. Two core characteristics were extracted in the proposed algorithm that involves the differences in traffic flow and of their position. The traffic flow was evaluated by the distance range among vehicles, whereas the position was evaluated using a semi-cooperative and voting filter mechanism. Further, two new classification mechanisms were used for relabeling the GHSOM units and for validating the GHSOM balance structure. The experiment has shown the supremacy of implemented IDS regarding stability, accuracy, message scales, and processing efficiency. The hierarchical relations need a lack of representation and the detection time needs more improvement.

In 2019, Ali et al. [26] have introduced an effective CL-PKS approach based on bilinear pairing to offer conditional privacy-preserving authentication for V2I communication in VANETs. In order to accelerate the verification process, the CL-PKS approach has supported the batch signature verification and aggregated the signature verification functions. Additionally, the blockchain was incorporated over the CL-PKS approach for the efficient implementation of revocation transparency of pseudo-identities before signature validation. Moreover, this approach has provided better protection and security against a diverse attack with less computational cost. V2V communication needs the CL-signature model for designing. It increases network congestion. The performance is bad for the long distance between source and destination.

In 2018, Hasrouny et al. [27] have implanted a novel security model based on vehicle behavior analysis. Moreover, an HTM and an MDS were defined that assigns a trust metric for each vehicle. The vehicle classification was made based on this trust metrics. The evaluation in terms of performance for HTM and MDS was performed using Groovenet Simulator. The outcomes have shown the effectiveness of the implemented approach on selecting the trustworthy vehicles and on monitoring their behaviors, further on classification and deactivation of malicious ones. The constraints, like specific frequent attacks and inter-group interaction need more improvement.

In 2019, Li et al. [28] have designed a new decentralized architecture named blockchain-based VANET based on blockchain technology. This process was comprised of four main phases: SBMs upload, blockchain set-up, vehicle registration, and blockchain record. In order to prevent the location and identity privacy, UGG, IPP, and LPP algorithms were proposed depending on k-anonymity unity and dynamic threshold encryption within the phases of SBMs upload. Further two indicators were introduced namely connectivity and average distance for quantifying the availability of k-anonymity unity. Experimental evaluation has been made for validating the efficiency of blockchain-based VANET and has shown superiority in terms of preventing identity and location privacy. It needs more energy. It is not a huge distributed computing system and it does not provide local network security.

2.2 Review

Table 1 explains the features and challenges of the state-of-the-art model on blockchain-based VANET models. Some of the features and challenges of the conventional models are explained as follows: PoW [22] efficiently used in VANET without storage overhead and effectively handles the trustworthiness. However, needs enhancement in the analysis to deal with crucial event message dissemination. Bayesian inference model [13] is effective and feasible for decentralized trust management and maintains a reliable and consistent database. The main drawback of this methodology is the need for Joint assurance of privacy preservation and trust management. BARS [23] has better transparency and conditional anonymity and poses improved robustness and efficiency, though, it is vulnerable to various attacks. Unified trust management [24] has enhanced data transmission and better effectiveness. It still needs enhancement over the security issues with virtualization and software-defined networking. I-GHSOM [25] poses quick and accurate detection of attacks and has fast extraction of distinct features from the message by vehicle. However, needs further improvement in overhead and detection time. CL-PKS [26] reduces the computational cost and performs efficiently in V2I communication. But, the designing of the CL-signature model for V2V communication is needed. HTM [27] has a better capability of vehicles to identify the effect of malicious users with improved trustworthiness. Future work needs by considering the constraints like specific frequent attacks and intergroup interaction. Blockchain-based VANET [28] has increased data processing time and offers high efficiency in privacy protection and system time, but it relies on trusted centralized entities.

3 VANET simulation and proposed trustability prediction and data hiding

This paper made an effort to introduce a new trust management solution in VANET. VANET is the same as the MANET yet has some modifications. VANET formed by a group of vehicles and roadside units RSU. Vehicles are named as OBU for data sharing or signal processing to and from RSUs. RSUs are defined as the installed units, which are fixed and this acts as the gateway for the communication among the servers or internet and OBU as well. VANET is seemed to be the most promising technology of Intelligent Transportation System (ITS) that helps in various services, and one among them is road safety service

Table 1 Features and challenges of state-of-the-art models on blockchain-based VANET

References	Methodology	Features	Challenges
Shrestha et al. [22]	PoW consensus mechanism	Efficiently used in VANET without storage overhead	Will enhance the analysis to deal with crucial event message dissemination
		Effectively handles the trustworthiness	
Yang et al. [13]	Bayesian inference model	Effective and feasible for decentralized trust management	Joint assurance of privacy preservation and trust management is needed
		Maintains a reliable and consistent database	
Liu et al. [23]	BARS	Better transparency and conditional anonymity	Vulnerable to various attacks
		Improved robustness and efficiency	
He et al. [24]	Unified trust management	Enhanced data transmission	Needs enhancement over the security issues with virtualization and software-defined networking
		Better effectiveness	
Liang et al. [25]	I-GHSOM	Quick and accurate detection of attacks	Needs further improvement in overhead and detection time
		Fast extraction of distinct features from the message by vehicle	
Ali et al. [26]	CL-PKS	Reduces the computational cost	Designing of CL-signature model for V2V communication is needed
		Perform efficiently in V2I communication	
Hasrouny et al. [27]	HTM	The better capability of vehicles to identify the effect of malicious users	Future work needs by considering the constraints like specific frequent attacks and intergroup interaction
		Improved trustworthiness	
Li et al. [28]	Blockchain-based VANET	Increased data processing time	Rely on trusted centralized entities
		High efficiency in privacy protection and system time	

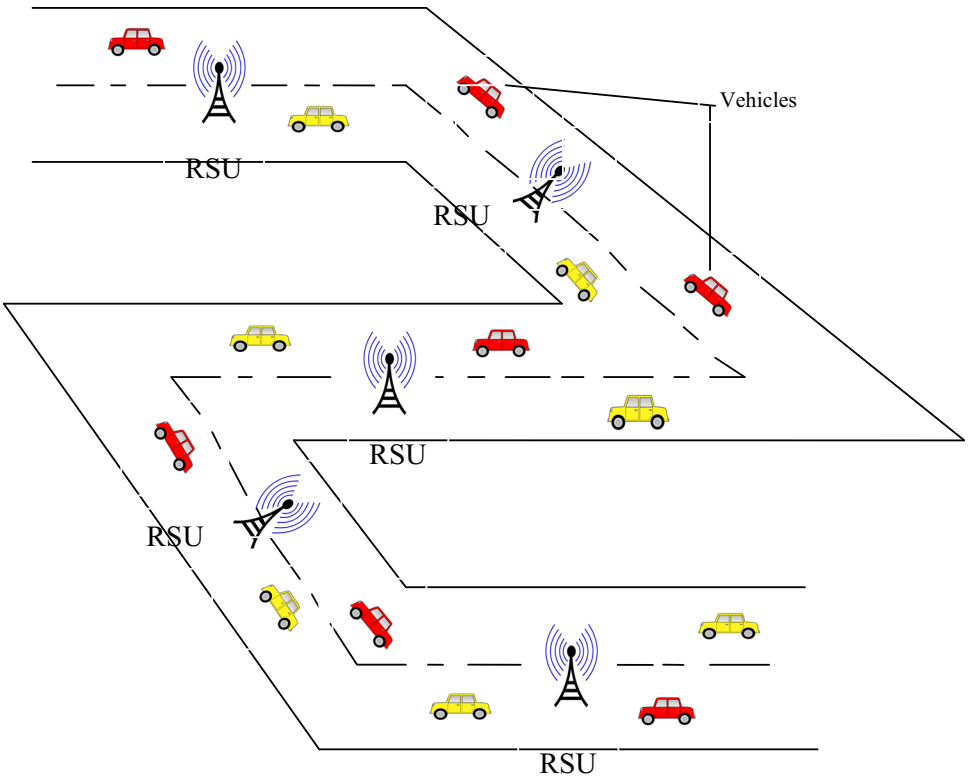

Fig. 1 General VANET architecture

that mainly focuses on minimizing road accidents via data sharing via the internet. Under this scenario, the security of data sharing among the vehicles is yet to be redefined, as the trust evaluation is a needed aspect. This paper aims to introduce a new trust management system in VANET with the involvement of blockchain technology. The simulation setup of the proposed VANET setup and processing is clearly described in Algorithm 1. Figure 1 exhibits the basic architecture of VANET.

3.1 System model

This section shows the system model of the proposed SLE-WOA. In Fig. 2 the data is sanitized before the transmission. From the sanitization the block chain storage is assisted to access model generated by the nodes. The VANET model consists of nodes that attempts to access message. A node then defines a number of properties as credentials. From the node the requested message is send to access the model. If the authentication is success then the

Algorithm 1: Proposed VANET simulation procedure and process

```
Define the count of vehicles, source vehicle, RSUs, VANET environment
while (t < sim_time)
                mobility mode ()
                if (t%T_s == 0)//in every T_s second, send
                data packets from source node and
                access by receiver node//
                send data()
                access data()
                authentication()
                provide access()
                End if
t=t+1
end while
```

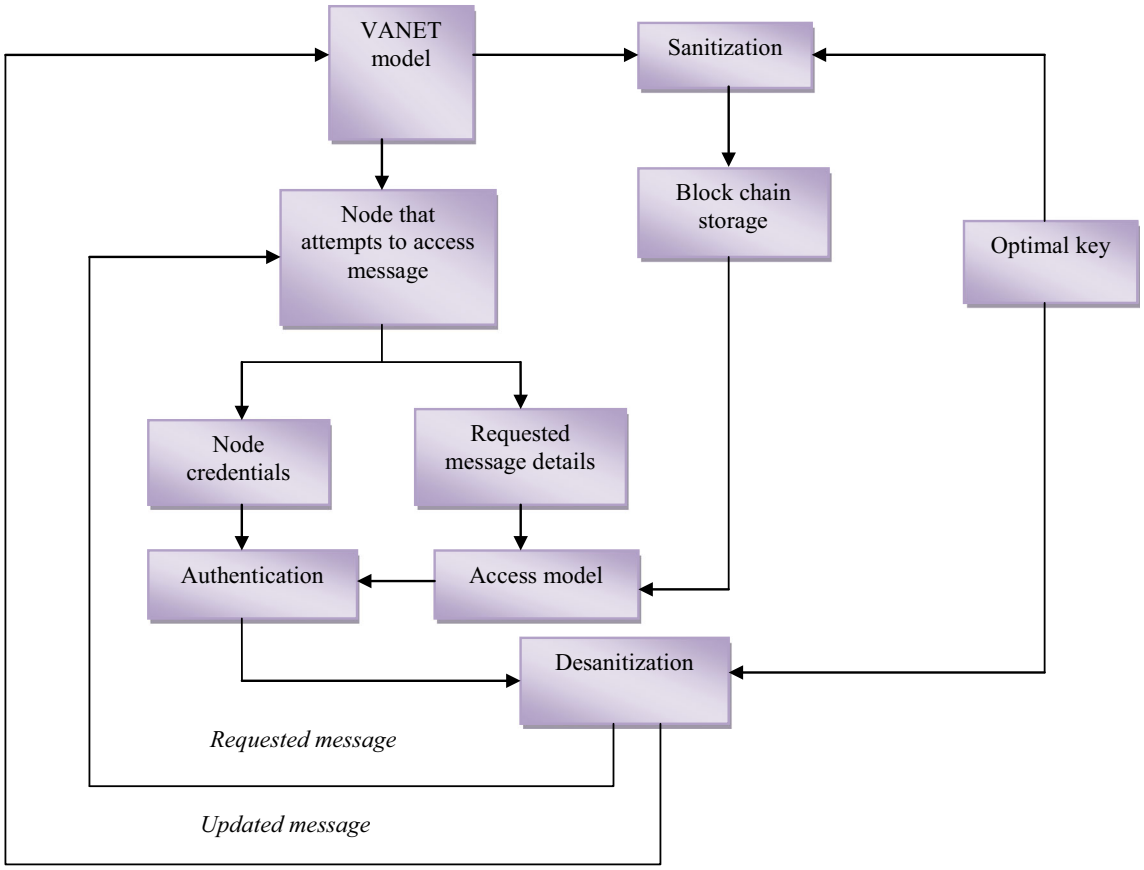

Fig. 2 The system model of the proposed SLE-WOA

desanitization takes place otherwise the above process is repeated until the authentication is success. The sanitization and desanitization is done using the optimal key.

3.2 Proposed architecture

Let us consider the vehicles $v_1, v_2, v_3 \ldots v_n$ moving under different RSUs. As the core work focuses on the secured VANET, message transmission is critically noticed to be safe. Hence, rather than passing the original message as it is, they are sanitized before transmission. The sanitization process emerges the privacy of data transmission while communication and the proposed sanitization process are explained in the subsequent section.

For the sanitization process, the key is the major requirement. Hence, the source that wants to broadcast message makes a key generation request to the respective RSU. This key generation optimistically takes place through an optimization algorithm, which is clearly explained in the further section. Further, the RSU maintains the key using blockchain technology. The sanitized data is broadcasted among vehicles and when the receiver is trying to access the message, it requests for the key to corresponding RSU. Before granting the key, RSU makes a trust evaluation to decide whether the node is authenticated or not. For this, a new logic of two-level trust evaluations is progressed in this paper, and it is given in the further section.

At each timestamp T_s, vehicle mobility alters the RSU coverage, and thereby the key request for the sanitization process happens accordingly. Moreover, all the RSUs are connected to the centralized server to which the keys (in the form of blocks) get shared. Figure 3 depicts the proposed architecture of trust evaluation based on VANET communication. The core advantage of this proposed work is summarized as follows:

- Original data is known only to the sender.
- The generated key is available with RSU. RSU authenticates receiver for data restoration.
- Only the sanitized data is transmitted among other vehicular nodes.

3.3 Data sanitization for secured message transmission with optimal key generation

Sanitization is considered as the data hiding process, in which the sensitive data are sanitized using a key K, which

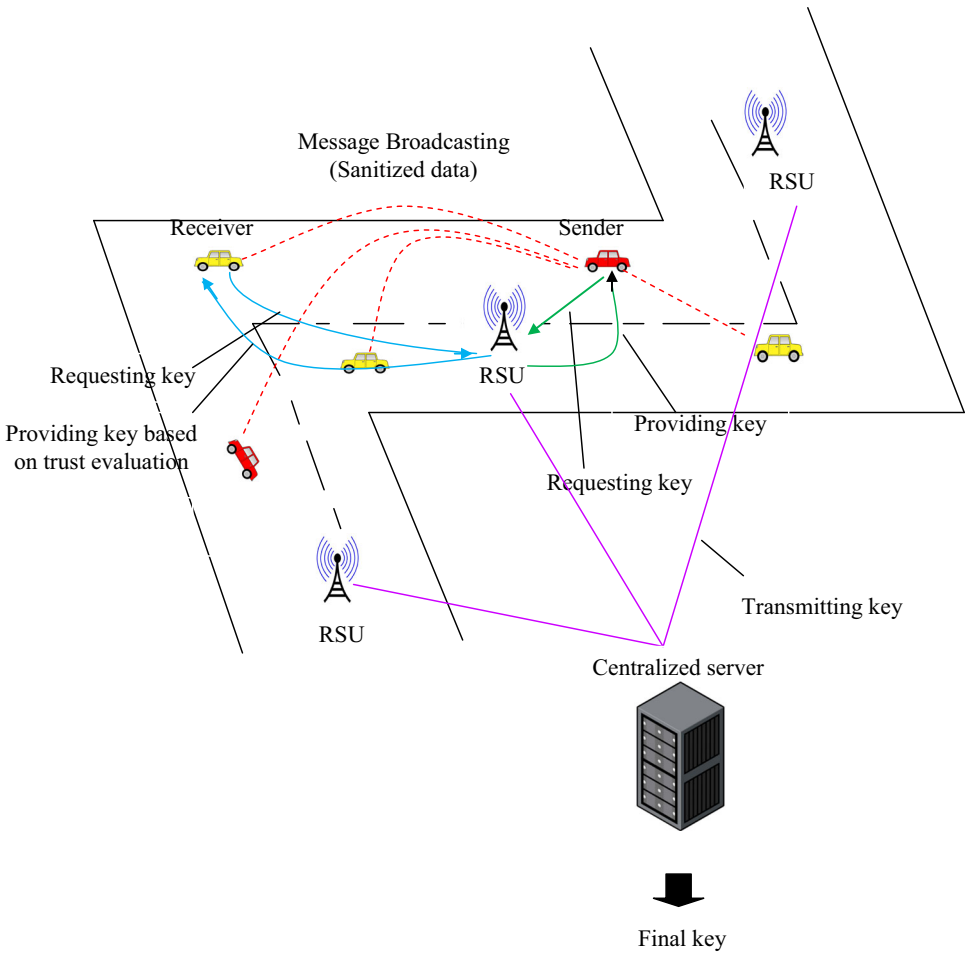

Fig. 3 Proposed architecture of trust evaluation based VANET communication

is arithmetically defined in Eq. (1). More importantly, the key plays a major role in the sanitization process, whose length is stated as key length = [Number of records × 1].

$$\hat{d} = d \oplus K \tag{1}$$

Moreover, the key should be optimal, and this paper introduces a new hybrid optimization algorithm for generating the optimal key in RSU. The hybrid algorithm is the hybridized form of SLnO and WOA, respectively. For instance: let us consider the data as $d_1 : [2 \quad 1 \quad 3]$, in which 1 is the sensitive data to be sanitized, the respective key is predicted as '2' and is XOR-ed with the sensitive data to generate the sanitized data. This working principle on the sanitization process is stated below in Fig. 4.

Therefore for d_1 (1), the sanitized data $\hat{d}$ is obtained as 3. The key generation process is made in two phases under the sender and RSU based on fitness function in Eq. (5). The process of optimal key generation is as follows: Initially, the sender request a key to RSU. Subsequently, the optimization process using the proposed hybrid algorithm

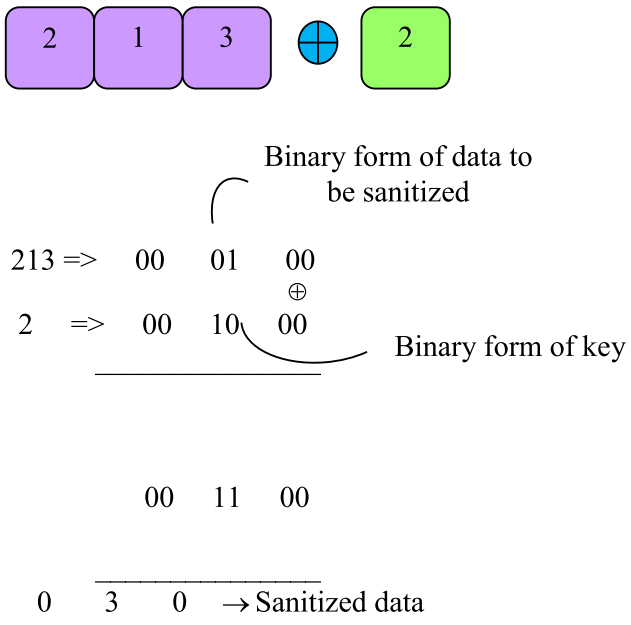

Fig. 4 Exemplary data with key

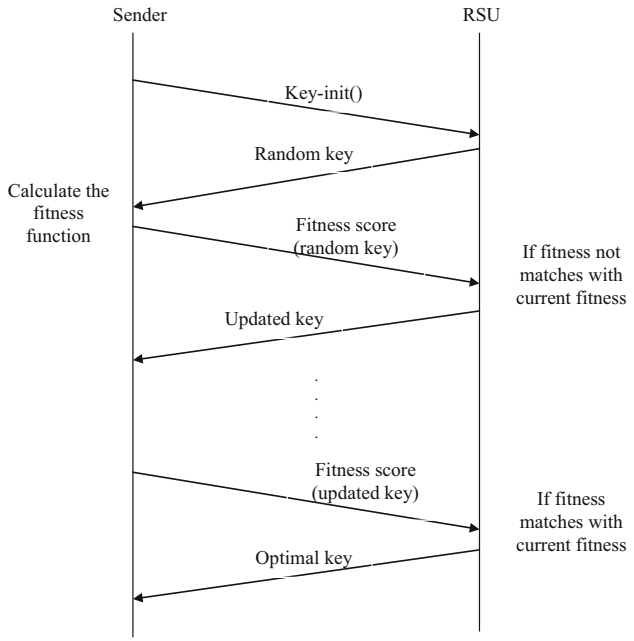

Fig. 5 Optimization-based key generation process

takes place in both sender and RSU and the process is as follows:

Population initialization: Once the key request is received, the RSU provides the random key to the Sender.

Fitness evaluation: The Sender evaluates the fitness (objective) to finalize the optimal key and the fitness score is send back to RSU.

Updating: If the fitness is attained, the key is kept as the optimal key and provide to the sender and in the else case (if the fitness is not attained), the key is updated and send to the sender for evaluating fitness again and gets the fitness score. The process continues to obtain the optimal key for sanitization.

Thus the final optimal key is provided to the sender. Figure 5 delineates the key generation process using the proposed algorithm.

In fact, blockchain technology is used to store the key into respective RSUs. Let us assume a scenario, the vehicle v_1 is under mobility, and at each Ts = 5, it transfers the message and hence it request the key to the respective RSU for sanitization process. As per Fig. 5, when Ts = 5, v_1 request K_1, which is stored in 1 of RSU 1. Then the key is also shared to neighbourhood RSU 2. When Ts = 10, v_1 is under RSU 2, and during message transmission, it requests the key to RSU 2 and it provides the same as well. Thereby, K_2 is stored along with K_1 as shown in Fig. 6. The Scenario of Key storage using BlockChain Technology is shown in Fig. 6. Then the generated key by RSUs is shared with a centralized server.

3.4 Data accessing by receiver

Once the sanitized message is broadcasted, the receiver vehicles try to access the data. To do this, the respective optimal key is required to access the original data and hence it gives key requests to RSU. However, RSU makes the trust evaluation to decide "whether to provide the key to the requesting vehicle". For this, a new trust evaluation process is introduced in this paper and once if the receiver is proved to be authenticated, it gets the key to access the original data by restoring it. If the RSU finds the requesting vehicle as unauthorized, it simply neglects its request.

3.5 Proposed trust evaluation process

This section explains the proposed trust evaluation process. To make the evaluation strong, the process goes out with two major levels:

1. Rule-based evaluation (Level 1)
2. Neural Network-based trust evaluation (Level 2)

Level 1: In this process, the receiver is subjected under the first level of evaluation to find whether the node (vehicle) is an intruder or not. This is continued by integrating some rule based evaluation, which is clearly explained below. Once if the condition under rule based evaluation gets unsatisfied, the evaluation process is forwarded to the NN model, where the behavior of node for PDR, PFR, and RSSI are trained already to know whether the node is authorized. Figure 7 explains the architecture of the proposed trust evaluation model.

Rule based trust evaluation: Here, the trustability of nodes are evaluated. Particularly, if the PDR, PFR and RSSI values of node v_i reach beyond the threshold value $\delta_{PDR_{Attack}}$, $\delta_{PFR_{Attack}}$ and $\delta_{RSSI_{Attack}}$, then the node is said to be malicious with the attack. Algorithm 2 explains the detection rules for various attacks.

Algorithm 2: Detection rules for diverse attacks

Input: PDR, PFR RSSI values of nodes $(ID-Node)$

Output: Detection of attack type

if $\begin{pmatrix}(PDR_{ID-Node} > \delta_{PDR}) \,\&\, (PFR_{ID-Node} > \delta_{PFR}) \,\&\\ (RSSI_{ID-Node} > \delta_{RSSI})\end{pmatrix}$ /*the node is subjected to DoS attack*/

send $Vote\_Message(attack, ID-Node)$ to RSU

else

send verification (ID-Node's RSSI, PDR, and energy level values, PDR of ID-Node's neighbouring nodes) message to RSU

end

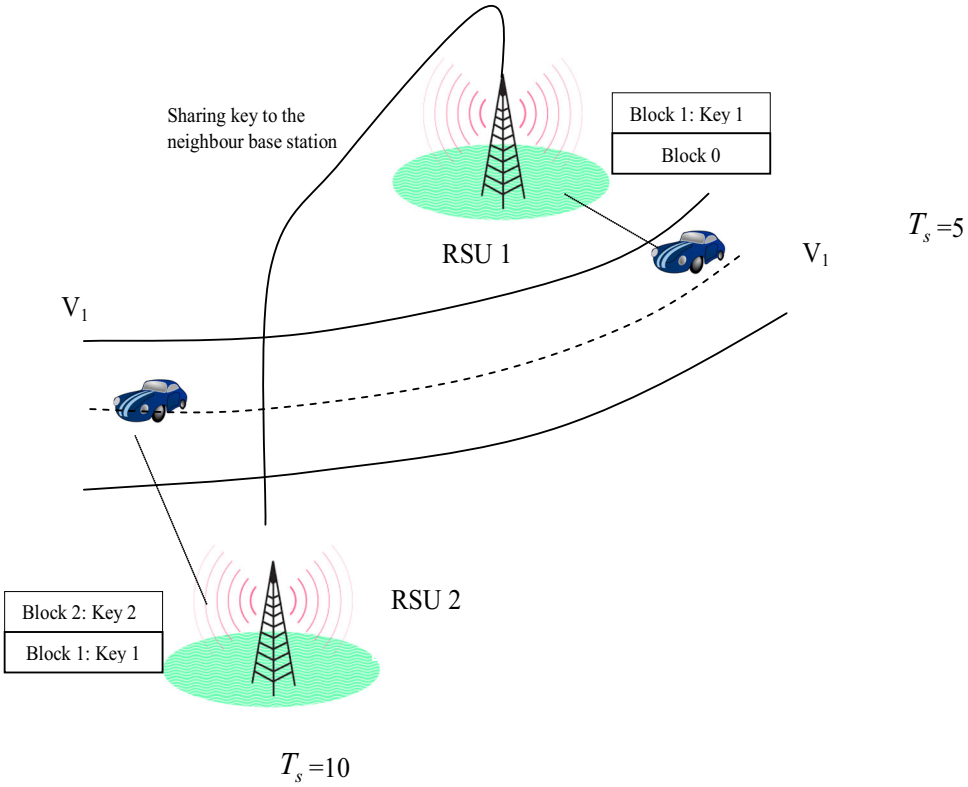

Fig. 6 Scenario of key storage using blockchain technology

Level 2: Once if the condition under level 1 is not satisfied, the evaluation is transferred to the next level (Level 2), where the NN model helps in detecting whether the node is authorized. Already the model is trained with the behavior of nodes for PDR, PFR, and RSSI, and at the time of testing, the trustability is predicted. The training library construction is illustrated in Table 2. The NN model [29] is as follows:

Equations (2), (3) and (4) explains the network model, in which $\dot{i}$ denotes the hidden neuron, $\hat{w}^{(o)}_{(\dot{i}k)}$ depicts the output weight from $\dot{i}^{th}$ hidden neuron to kth layer, $IN_{(n)}$ portrays the input neuron's count, $HI_{(n)}$ signifies the hidden neuron's count, $\hat{w}^{(HI)}_{(\tilde{b}\dot{i})}$ exhibits the bias weight to $\dot{i}^{th}$ hidden neuron, $\hat{w}^{(HI)}_{(l\dot{i})}$ delineates the weight from lth input to $\dot{i}^{th}$ hidden neuron, $\hat{w}^{(o)}_{(\tilde{b}k)}$ expresses the output bias weight to kth layer, and NF terms as the activation function. $\overline{OU}_k$ is stated as the network output, predicted output and it is demonstrated in Eq. (3), OU_k is portrayed as actual output.

$$\overline{HO}^{(HI)} = NF\left(\hat{w}^{(HI)}_{(\tilde{b}\dot{i})} + \sum_{l=1}^{IN_{(n)}} \hat{w}^{(HI)}_{(l\dot{i})}(Inputfeatures)\right) \tag{2}$$

$$\overline{OU}_k = NF\left(\hat{w}^{(o)}_{(\tilde{b}k)} + \sum_{\dot{i}=1}^{HI_{(n)}} \hat{w}^{(o)}_{(\dot{i}k)} \overline{HO}^{(HI)}_{\dot{i}}\right) \tag{3}$$

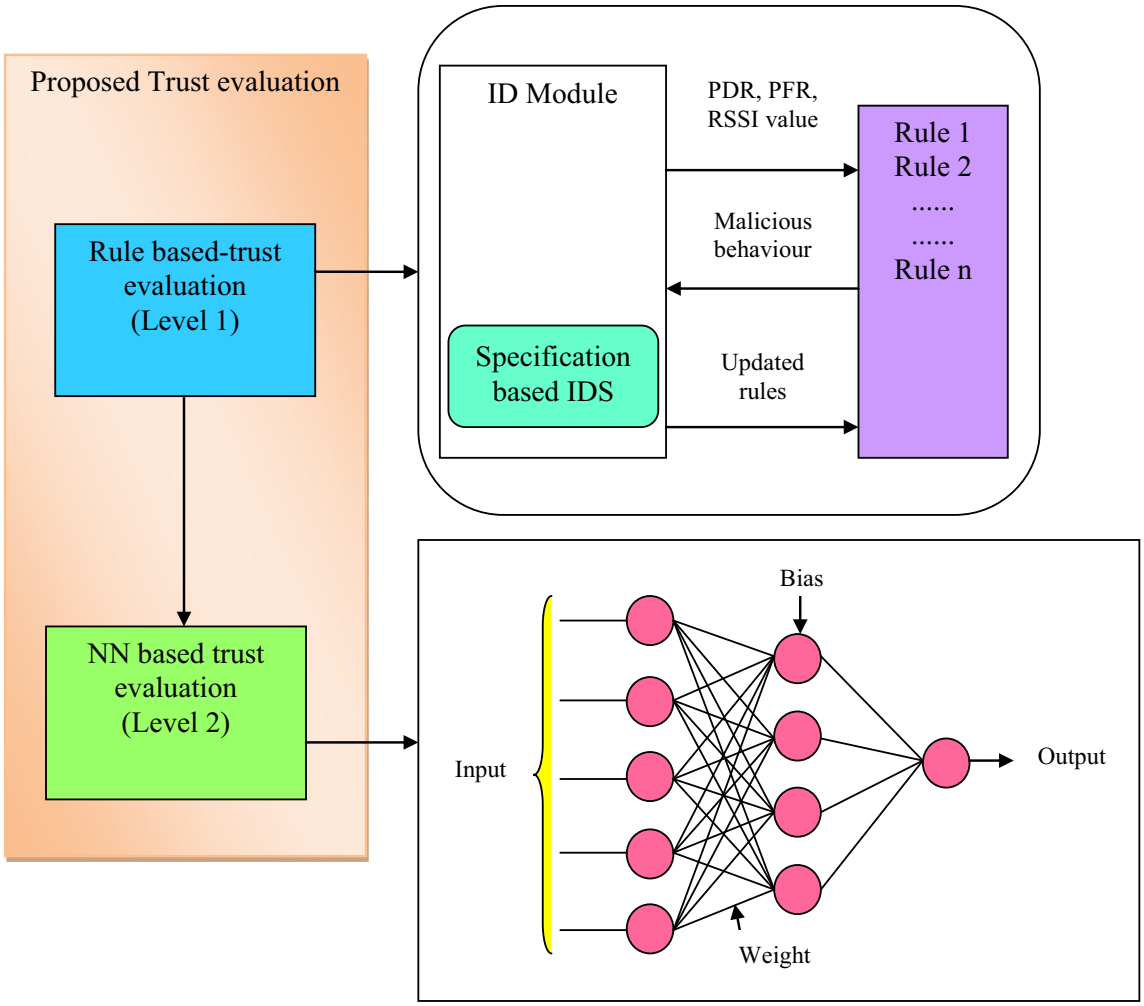

Fig. 7 Architecture of proposed trust evaluation process

Table 2 Training library construction

Node	PDR	PFR	RSSI	Label (0/1) (authorized node or not)
v_1	–	–	–	–
v_2	–	–	–	–
…	–	–	–	–
…	–	–	–	–
v_N	–	–	–	–

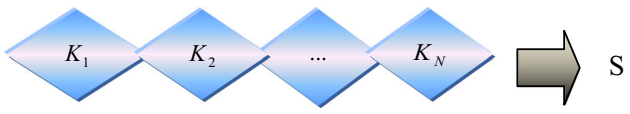

Fig. 8 Solution encoding of proposed model

$$ER^* = \underset{\left\{\hat{w}_{(bi)}^{(HI)},\hat{w}_{(li)}^{(HI)},\hat{w}_{(bk)}^{(o)},\hat{w}_{(ik)}^{(o)}\right\}}{\arg\min} \sum_{k=1}^{O_{(n)}} |OU_k - \overline{OU}_k| \quad (4)$$

4 Optimal key by hybrid algorithm: combination of SLnO and WOA models

4.1 Objective function and solution encoding

The objective function of the proposed VANET simulation approach is exploited as per Eq. (5). The solution encoding that given as input to the proposed model is illustrated as per Fig. 8.

$$Obj = \min(O) \tag{5}$$

where

$$O = \left(\frac{1}{HR}\right) + sum(DR) \tag{6}$$

$$HR = \frac{No\ of\ sensitive\ data\ hidden\ successfully}{Total\ no\ of\ sensitive\ data} \tag{7}$$

$$DR = abs(original\,data - sanitized\ data) \tag{8}$$

4.2 Sea Lion Optimization Algorithm

SLnO [30] algorithm is the renowned optimization algorithm developed based on the hunting behavior of Sea lions. The sea lions have posed few attractive features such as fast movement, clear vision, and superior hunting property. Sea lions further have interesting sensitive features named Whiskers which supports them to determine the correct prey position. These whiskers are useful for sea lions to express the position, shape, and size of prey. On considering their hunting behavior, the main phases in sea lions are

- Tracking and chasing of prey by their whiskers.
- Pursuing and encircling the prey by calling other members of their subgroups to join them.
- Attack the prey.

Mathematical modeling: The SLnO algorithm is arithmetically defined with four phases called tracking, social hierarchy, attacking and encircling prey.

Detecting and tracking phase: The whiskers support the sea lion to sense the existing prey and to detect their position. This is made while the direction of whiskers is against the water wave's direction. Although, the vibration of whiskers is fewer as its orientation is on the same present orientation.

Sealion discovers the prey's position and invites other members to unite its subgroup for chasing and hunting the prey. The leader among that sea lion is the one who calls others and the position update of target prey is handled by other members. This algorithm assumes the target prey as the one that is closer to the optimal solution or presents the best solution. This behavior is arithmetically expressed as per Eq. (9), in which the distance among the sea lion and target prey is explained as $\overrightarrow{Dis}$, the vector position of sea lion and target prey is indicated as $\vec{S}(t)$ and $\vec{M}(t)$, respectively, t is the present iteration and the random vector is expressed as $\vec{G}$.

$$\overrightarrow{Dis} = \left|2\vec{G}.\vec{M}(t) - \vec{S}(t)\right| \tag{9}$$

In the subsequent iteration, the sea lion shifts over the target prey to get closer. The arithmetical modeling of this behavior is expressed using Eq. (10), in which the next iteration is given by $(t+1)$ and $\vec{H}$ gets decreased gradually over an iteration course to 2 from 0.

$$\vec{S}(t+1) = \vec{M}(t) - \overrightarrow{Dis}.\vec{H} \tag{10}$$

Vocalization phase: Sea lions can endure both in land and water. On comparing the sea lions sound, the sound in air is moved four times faster than the sound in land. While on prey hunting, the communication of sea lions is made via several vocalizations. Furthermore, they pose the capability of identifying the sound both on and under the water. Hence, after identified prey, the sea lion invites the other members for prey's encircling and attacking. This is arithmetically computed as per Eqs. (11), (2) and (13), in which the speed of sea lion leader's sound is depicted as $\overrightarrow{S_{leader}}$, the sounds speed in water and air is symbolized as $\overrightarrow{P_1}$ and $\overrightarrow{P_2}$.

$$\overrightarrow{S_{leader}} = \left|\left(\overrightarrow{P_1}(1 + \overrightarrow{P_2})\right)/\overrightarrow{P_2}\right| \tag{11}$$

$$\overrightarrow{P_1} = \sin\theta \tag{12}$$

$$\overrightarrow{P_2} = \sin\varphi \tag{13}$$

Attacking phase: In the exploration phase, two stages are exploited under the sea lions hunting behavior and are exhibited as follows:

(a) *Dwindling encircling approach:* This approach is based on $\vec{F}$ *the* value in Eq. (10). Largely, $\vec{F}$ value is decreased progressively via a course of iteration from 2 to 0. This decreasing factor directs the sea lion to forward on and to encircle the prey.

(b) *Circle updating position:* The bait ball of fishes is chased and attacked by sea lion from edges and is stated as per Eq. (11), in which the distance among the search agent (sea lion) and best optimal solution (target prey) is given as $\vec{M}(t) - \vec{S}(t)$ the absolute value is exploited as $\|$ and the random number is explained as l and is falls between -1 and 1.

$$\vec{S}(t+1) = \left|\vec{M}(t) - \vec{S}(t).\cos(2\pi l)\right| + \vec{M}(t) \tag{14}$$

Prey searching: Based on the best search agent in the exploration part, the position update of the sea lion is formulated. The search agent's position update within the exploration phase is exploited in compliance to the chosen random sea lion. It is further said as, the SLnO algorithm performs a global search agent and identifies the global

optimum solution, while $\overrightarrow{F}$ is larger than 1. This is explained using Eqs. (15) and (16).

$$\overrightarrow{Dis} = \left|2\overrightarrow{B}.\overrightarrow{S_{rnd}}(t) - \overrightarrow{S}(t)\right| \tag{15}$$

$$\overrightarrow{S}(t+1) = \overrightarrow{S_{rnd}}(t) - \overrightarrow{Dis}.\vec{H} \tag{16}$$

4.3 Whale Optimization Algorithm

WOA [31] is the renowned optimization concept based on humpback whales' bubble-net feeding behavior. The mathematical demonstration of WOA is exhibited in the following:

Shrinking encircling mechanism: The prey's current position is identified at the time of hunting course by whales. After that, the prey is encircled by them. The target prey is assumed as the recent best solution; next to this, the position gets updated for attaining the optimal solution. The whale's encircling behaviour is explicated as per Eqs. (17) and (18).

$$\vec{F} = \left|\vec{W}.\vec{S}^{*}(t) - \vec{S}(t)\right| \tag{17}$$

$$\vec{S}(t+1) = \vec{S}^{*}(t) - \vec{H}.\vec{F} \tag{18}$$

In which, the present iteration is depicted as t, the best solution's position vector is signified as S^{*}, the coefficient vectors are expressed as H and W, and the vector's position is portrayed by S, the element-by-element multiplication is enabled based on "." Function and the absolute value is stated as ||. S^{*} needs to be updated if they exist the best solution. The vectors H and W are evaluated as per Eqs. (19) and (20).

$$\vec{H} = 2\vec{s}.\vec{x} - \vec{s} \tag{19}$$

$$\vec{W} = 2\vec{x} \tag{20}$$

In which, the s value addresses a gradual reduction that lies between 2 and 0 and a random vector x is designated to have the range [0, 1].

Spiral updating position: The position update among the prey and humpback whale is computed numerically using the spiral equation in Eqs. (21) and (22).

$$\vec{F} = \left|\vec{S}^{*}(t) - \vec{S}(t)\right| \tag{21}$$

$$\vec{S}(t+1) = \vec{F}'.e^{dz}.(\cos 2\pi z) + \vec{S}^{*}(t) \tag{22}$$

In this, the logarithmic spiral's shape is explained based on d and is considered to be a constant, and the random number is exploited by z and is spread out constantly between − 1 and 1. The numerical modeling of probability estimation is performed using Eq. (23), in which every feasible path for encircling is denoted as pb.

$$\begin{aligned} \vec{S}(t+1) &= \vec{S}^{*}(t) - \vec{H}.\vec{F} && \text{if } pb < 0.5 \\ \vec{S}(t+1) &= \vec{F}'.e^{dz}.(\cos 2\pi z) + \vec{S}^{*}(t) && \text{if } pb \geq 0.5 \end{aligned} \tag{23}$$

Moreover, the random value H plays its major role in the global updating of the search agent. Equations (24) and (25) defines the mathematical formulation of this WOA theory. In Eq. (25), $\vec{S}_{rad}$ is decided as an arbitrary value from the whales during the current tryout run.

$$\vec{F} = \left|\vec{W}.\vec{S}_{rad} - \vec{S}(t)\right| \tag{24}$$

$$\vec{S}(t+1) = \vec{S}_{rad} - \vec{H}.\vec{F} \tag{25}$$

4.4 Proposed algorithm

The WOA is the recently developed nature-inspired approach that imitates the hunting characteristics of humpback whales, whereas the SLnO algorithm has initiated based on the sea lions hunting behaviour in nature. Both these algorithm has attained better performance in many terms yet suffers from premature convergence that impacts them to trap in local optima. Hence, this paper tries to implement a new improved algorithm by hybridizing these two algorithms (WOA + SLnO). For this, the SLnO concept is incorporated inside the WOA algorithm and is thus named as SLE-WOA. Here, the exploration phase of a sea lion in Eq. (16) is considered for this hybridization. In the conventional WOA algorithm, when the probability $pb < 0.5$, two conditions are evaluated, one is if $|H| < 1$, the position update is computed using Eq. (17) on other conditions $|H| \geq 1$, the position update is computed based on Eq. (22). In this proposed work, the modification is formulated over the condition $|H| \geq 1$, where the update equation of WOA is replaced by the sea lion equation given in Eq. (14). The pseudo-code of the implemented SLE-WOA algorithm is explained in Algorithm 3. The flowchart of the proposed SLE-WOA approach is depicted in Fig. 9.

Algorithm 3: Pseudocode of Proposed SLE-WOA algorithm

```
Initiate the whale population S_i (i = 1,2,....,n)
Evaluate the fitness of every search agent
S* = best search agent
While (t < max iteration)
        For every search agent
                Update s, H, F, z and pb
                if (pb < 0.5)
                        if (|H| < 1)
                                Update the present search agent position by Eq. (17)
                        Else if
                                Choose the arbitrary search agent (S_rad)
                                Update the present search agent position on the basis of the
                                exploration equation of sea lion in Eq(14)
                        End if
                Else if
                                Update the current search position by Eq. (25)

                End if
        End for
        Verify if any search agent leave afar the search
        space and modify it
        Estimate the fitness of every search agent
        Update S* as per the best solution
t=t+1
End while
return S*
```

5 Results and discussions

5.1 Simulation setup

The implemented trust management system was implemented in MATLAB. The dataset used for evaluating the trustability of the node is the KDDcup dataset. The certain analysis is performed to prove the betterment proposed work:

- The analysis of proposed work is carried out for certain attacks like KCA and CCA attacks, KPA and CPA attacks along with rejection ratio and key sensitivity, respectively.
- Further, the analysis of the NN classifier is performed over other state-of-the-art classifiers like SOM [32] and GHSOM [33] with respect to sensitivity, specificity, accuracy, and precision, FPR, FDR, FNR, MCC, F1-score and NPV.
- The analysis gets extended by comparing the implemented hybrid algorithm to other classical models like WOA [31], SLnO [30], GA [34] and DA [35].
- Further, the analysis has been performed for the proposed and Conventional Models, such as WOA [31], SLnO [30], GA [34], and DA [35] by considering KPA and CPA attack.
- Further, the performance of the NN Model in Trustability Prediction is performed over the classifiers like SOM [32], GHSOM [33], and NN [29] with respect to Accuracy, Sensitivity, Specificity, Precision, FPR, FNR, NPV, FDR, F1_score, and MCC.

5.2 Analysis of rejection ratio

Figures 10 and 11 shows the count of nodes get rejected by proposed work under both the rule based and NN based scenario. The formulation of the rejection ratio is defined in Eq. (26). Moreover, the analysis (number of rejections) is made for each time stamps. While analyzing, more rejections have been done under NN based trust evaluation. More particularly, at the 4th timestamp, T_s = 20, 100% of the node that subjected to the NN model for trust prediction is rejected, which shows that the nodes are malicious. Similarly, the rejection ratio at each time stamps is plotted in the graph.

$$\text{Rejection ratio} = \frac{No\ of\ rejections}{No\ of\ attempts} \tag{26}$$

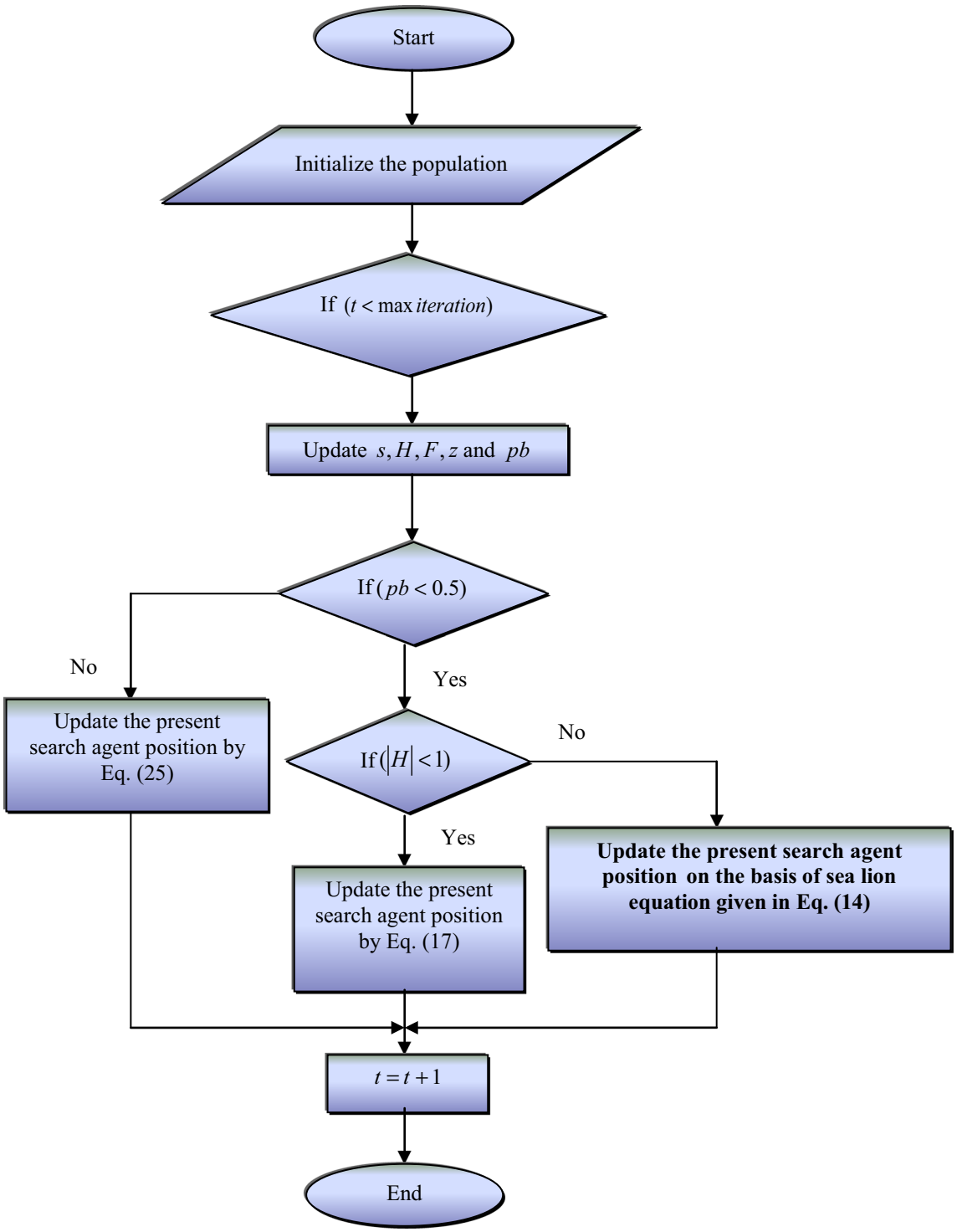

Fig. 9 Flowchart of proposed SLE-WOA algorithm

5.3 Analysis on KCA and CCA attack

This section explains the robustness of proposed work against KCA and CCA attack. In the known ciphertext attack, the attacker has the access merely to a set of ciphertexts, yet has some knowledge of the plaintext. Under this analysis, it is reported that the implemented model is robust against the KCA attack. In this, the analysis is performed by varying the percentage of plaintext data and the outcomes are obtained and are symbolized in Table 3. The proposed SLE-WOA algorithm by varying the plaintext as 5% has proved its robustness against the

KCA attack with less possibility of retrieving the original data.

Subsequently, "a CCA is an attack model for cryptanalysis in which the cryptanalyst gathers information, at least in part, by choosing a ciphertext and obtaining its decryption under an unknown key". In this, the analysis is carried out by varying the percentage of ciphertext data and the outcomes are obtained and are given in Table 4. By varying the ciphertext to different percentage levels, the proposed model is proved for its efficiency over avoiding CCA attack.

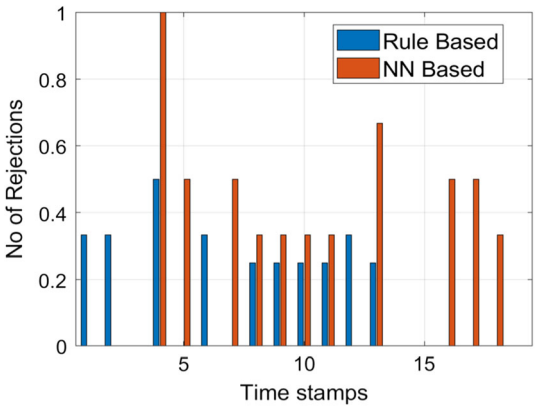

Fig. 10 Analysis of rejection ratio: Level 1 and Level 2

5.4 Analysis on KPA and CPA attacks

This section explains the robustness of proposed work against KPA and CPA attack. The ciphertext and its respective plaintext in known-plaintext attacks can be easily accessed by the attacker. The major goal is on predicting the secret key (or the secret key count). Under this analysis, it is observed that the implemented approach is greatly robust against the KPA attack as the attacker cannot gain the original data. From Table 5, it is observed that the attacker could access only 71% of original data and thus it failed in its attempt to get the original data. Similarly during CPA, the attacker can decide the plaintext records randomly for encryption and based on that, achieves the respective ciphertext. He made an attempt to purchase the secret key for encryption or alternatively to generate an approach that might permit him to decrypt some ciphertext messages that encrypted utilizing this key (with no detail about the secret key). Table 5 shows how the proposed algorithm is robustness to CPA attack when compared to other conventional models. During this attack, only 70% of the original message is acquired by the attacker.

5.5 Key sensitivity analysis

In this section, the robustness of the sanitization key is investigated by varying the sanitization key to 5%, 10%, 15%, and 20%, respectively and attempted to recover the

Fig. 11 Optimal key generated by RSUs using WOA

RSU 1	
Key 5	<4,1,1,3,5>
Key 4	<1,3,6,3,5>
Key 3	<2,5,1,7,7>
Key 2	<4,6,3,1,1>
Key 1	<3,5,5,3,1>

RSU 2	
Key 13	<1,1,7,6,3>
Key 12	<4,3,2,3,9>
Key 11	<1,5,1,7,3>
Key 10	<1,7,8,1,1>
Key 9	<3,8,1,1,6>
Key 8	<6,2,7,1,1>
Key 7	<5,2,1,7,6>
Key 6	<3,3,2,1,5>

RSU 3	
Key 19	<2,3,3,3,1>
Key 18	<1,3,2,4,3>
Key 17	<4,2,1,4,7>
Key 16	<1,3,3,6,4>
Key 15	<2,1,9,4,7>
Key 14	<3,1,5,4,4>

Table 3 Analysis on KCA attack: proposed over conventional models

Varying the plaintext	WOA [31]	SLnO [30]	GA [34]	DA [35]	SLE-WOA
per_5	0.72171	0.94183	0.74796	0.81475	0.71012
per_10	0.7862	0.95587	0.79836	0.80685	0.78312
per_15	0.78387	0.95203	0.79205	0.80255	0.77692
per_20	0.78532	0.94731	0.81127	0.80674	0.77895
per_25	0.82122	0.9574	0.84862	0.83123	0.81308

Table 4 Analysis on CCA attack: proposed over conventional models

Varying the ciphertext	WOA [31]	SLnO [30]	GA [34]	DA [35]	SLE-WOA
per_5	0.74726	0.93655	0.82058	0.78959	0.71805
per_10	0.77919	0.94739	0.82984	0.79913	0.73357
per_15	0.83901	0.95472	0.86073	0.85565	0.78566
per_20	0.86913	0.95923	0.87249	0.88676	0.8209
per_25	0.87897	0.96325	0.87299	0.89539	0.85283

Table 5 Analysis on KPA and CPA attack: proposed and conventional models

	KPA	CPA
WOA [31]	0.72171	0.77448
SLnO [30]	0.94183	0.9055
GA [34]	0.74796	0.73534
DA [35]	0.81475	0.75548
SLE-WOA	0.71012	0.71106

Table 6 Key sensitivity analysis

	WOA [31]	SLnO [30]	GA [34]	DA [35]	SLE-WOA
per_5	0.34343	0.3942	0.45439	0.47096	0.23084
per_10	0.23832	0.41433	0.31735	0.4506	0.17537
per_15	0.24754	0.41131	0.3149	0.43664	0.16612
per_20	0.25011	0.37802	0.32338	0.41904	0.15964
per_25	0.29927	0.40266	0.31205	0.40839	0.16066

original data (Table 6). The resultant data is compared to the original data. While analyzing, it is observed that the implemented sanitization model can produce only 17% of original data with 10% of the key variation. However, the key with a variation of the conventional method has retrieved 40% of original data. A similar analysis is made for all the remaining variation. Table 6 shows the key sensitivity analysis.

5.6 Analysis on classifier

The proposed work uses the NN model for predicting the trustability of nodes, and the performance of the classifier is analyzed over other state-of-the-art methods like models SOM and GHSOM. In fact, the analysis is carried out under both positive and negative measures. From Table 7, it is observed that the prediction accuracy of NN is 92%, whereas the conventional methods show its poor performance with less accuracy.

$$Accuracy = \frac{(TP + TN))}{(TP + TN + FP + FN)} \tag{27}$$

Similarly, the FPR by NN is least (0.08) when compared over other models, which shows that it is 16.33% and 15.1% superior to SOM and GHSOM, respectively. The performance evaluation formula is defined in Eq. (28).

$$perf\ \% = \frac{proposed - conventional}{conventional} \times 100 \tag{28}$$

Further, the overall trustability prediction results in Table 8 shows that: as the rule based and NN based models are combined to evaluate the trustability of node, the proposed trust management system is strong enough to control the malicious activity in the network, which is proved using certain positive and negative measures.

Table 7 Performance of NN model in trustability prediction

	SOM [32]	GHSOM [33]	NN [29]
Accuracy	0.74576	0.89831	0.92308
Sensitivity	0.38889	0.85714	1
Specificity	0.90244	0.90385	0.91837
Precision	0.63636	0.54545	0.42857
FPR	0.097561	0.096154	0.081633
FNR	0.61111	0.14286	0
NPV	0.90244	0.90385	0.91837
FDR	0.36364	0.45455	0.57143
F1_score	0.48276	0.66667	0.6
MCC	0.34442	0.63185	0.62736

Table 8 Overall performance analysis

	Rule-based	NN-based	Overall performance
Accuracy	0.83051	0.92308	0.88136
Sensitivity	0.57143	1	0.7
Specificity	0.86538	0.91837	0.91837
Precision	0.36364	0.42857	0.63636
FPR	0.13462	0.081633	0.081633
FNR	0.42857	0	0.3
NPV	0.86538	0.91837	0.91837
FDR	0.63636	0.57143	0.36364
F1_score	0.44444	0.6	0.66667
MCC	0.36268	0.62736	0.5957

5.7 Representation of key management in RSU via blockchain technology

Figures 10, 11, 12, 13, 14 and 15 shows how the optimal key generated by RSUs is stored in blocks. This shows the mobility of the vehicle in each time stamps and the key generation in each RSU (RSU 1, 2, and 3) to the requesting vehicle. Moreover, the section reveals how the generated optimal keys are maintained in each RSU through blocks (both proposed and conventional models).

Fig. 12 Optimal key generated by RSUs using SLnO

RSU 1	
Key 5	<1,3,2,1,1>
Key 4	<1,1,3,1,7>
Key 3	<3,1,1,1,1>
Key 2	<1,1,1,1,1>
Key 1	<3,1,1,1,1>

RSU 2	
Key 13	<1,3,1,1,1>
Key 12	<1,3,1,3,1>
Key 11	<1,1,1,1,2>
Key 10	<1,3,1,1,1>
Key 9	<1,1,1,1,3>
Key 8	<1,1,1,1,2>
Key 7	<1,1,1,3,3>
Key 6	<1,1,1,1,2>

RSU 3	
Key 19	<1,1,1,1,2>
Key 18	<1,7,1,3,1>
Key 17	<1,1,1,5,1>
Key 16	<1,1,2,3,1>
Key 15	<1,1,1,2,1>
Key 14	<1,1,1,1,1>

Fig. 13 Analysis on optimal key that generated by RSUs using GA

RSU 1	
Key 5	<8,5,5,3,3>
Key 4	<6,5,1,2,7>
Key 3	<1,1,1,5,3>
Key 2	<5,1,1,3,2>
Key 1	<6,1,1,3,1>

RSU 2	
Key 13	<3,2,1,2,7>
Key 12	<6,2,2,2,7>
Key 11	<1,3,3,3,8>
Key 10	<3,1,2,5,5>
Key 9	<7,3,5,1,3>
Key 8	<1,2,6,2,2>
Key 7	<1,3,5,4,3>
Key 6	<6,5,7,1,1>

RSU 3	
Key 19	<3,6,2,7,1>
Key 18	<2,7,2,1,8>
Key 17	<4,6,6,6,6>
Key 16	<3,4,2,5,4>
Key 15	<1,3,3,2,6>
Key 14	<3,4,3,3,5

Fig. 14 Optimal key generated by RSUs using DA

RSU 1	
Key 5	<1,5,7,3,4>
Key 4	<1,7,5,1,1>
Key 3	<3,6,3,6,6>
Key 2	<5,2,7,7,5>
Key 1	<2,1,3,3,1>

RSU 2	
Key 13	<8,3,3,1,7>
Key 12	<1,3,1,1,1>
Key 11	<2,3,1,5,3>
Key 10	<3,6,5,3,3>
Key 9	<1,4,3,7,5>
Key 8	<3,5,3,7,6>
Key 7	<7,3,3,6,3>
Key 6	<1,3,3,1,5>

RSU 3	
Key 19	<7,7,1,2,3>
Key 18	<1,3,7,2,9>
Key 17	<2,3,6,1,6>
Key 16	<3,3,1,3,3>
Key 15	<3,6,1,4,1>
Key 14	<3,3,5,3,3>

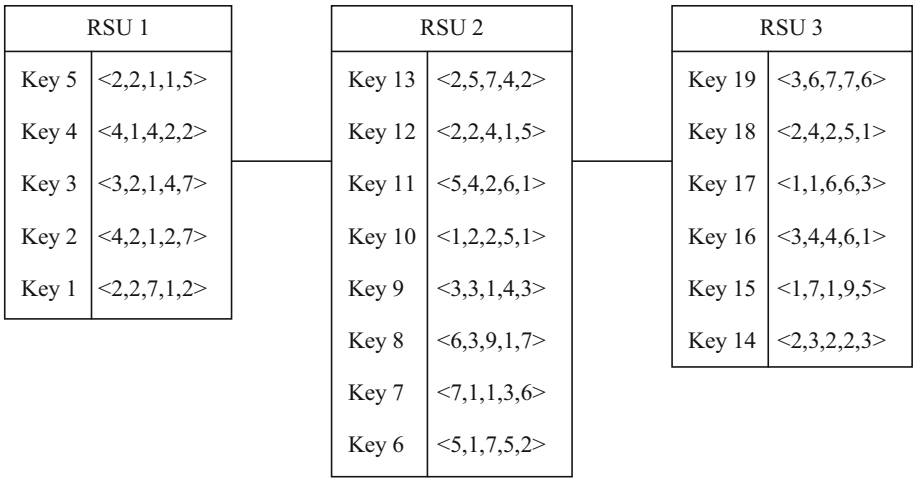

Fig. 15 Optimal keys generated by RSUs using proposed SLE-WOA algorithm

6 Conclusion

This research work has introduced a novel trust management system in VANET with two main phases: Secured Message Transmission and Node Trustability Prediction. The security assured message passing was performed by integrating the privacy preservation model under the Data Sanitization process. Furthermore, the optimization concept operated as a major role, in which the key utilized for the sanitization process was optimally tuned using a novel hybrid algorithm named SLE-WOA, which is the combination of WOA and SLnO algorithm, respectively. Subsequently, the trustability of the node was computed based on the "two-level evaluation process" i.e., rule based and machine learning-based evaluation process. To the end, the proposed model regarding performance was validated against other classical models in terms of certain measures. The result thus analyzed that the proposed sanitization method in terms of key sensitivity analysis can produce only 17% of original data with 10% of the key variation. However, the key with a variation of the conventional method has retrieved 40% of original data.

References

1. Kumar, A., & Gupta, M. (2018). A review on activities of fifth generation mobile communication system. *Alexandria Engineering Journal, 57*(2), 1125–1135.
2. Mukherjee, A., & De, D. (2016). Femtolet: A novel fifth generation network device for green mobile cloud computing. *Simulation Modelling Practice and Theory, 62,* 68–87.
3. Feijóo, C., Gómez-Barroso, J. L., & Ramos, S. (2016). Techno-economic implications of the mass-market uptake of mobile data services: Requirements for next generation mobile networks. *Telematics and Informatics, 33*(2), 600–612.
4. Habbal, A., Goudar, S. I., & Hassan, S. (2019). A context-aware radio access technology selection mechanism in 5G mobile network for smart city applications. *Journal of Network and Computer Applications, 135,* 97–107.
5. Benrhaiem, W., & Hafid, A. S. (2019). Bayesian networks based reliable broadcast in vehicular networks. *Vehicular Communications*, *21*, 100181.
6. Urra, O., & Ilarri, S. (2019). Spatial crowdsourcing with mobile agents in vehicular networks. *Vehicular Communications, 17,* 10–34.
7. Osman, R. A., Peng, X. H., & Omar, M. A. (2019). Adaptive cooperative communications for enhancing QoS in vehicular networks. *Physical Communication, 34,* 285–294.
8. Hussain, R., Hussain, F., & Zeadally, S. (2019). Integration of VANET and 5G security: A review of design and implementation issues. *Future Generation Computer Systems, 101,* 843–864.
9. Hasrouny, H., Samhat, A. E., Bassil, C., & Laouiti, A. (2019). Detection and efficient revocation within VANET. *Journal of Information Security and Applications, 46,* 193–209.
10. Arif, M., Wang, G., Bhuiyan, M. Z. A., Wang, T., & Chen, T. (2019). A survey on security attacks in VANETs: Communication, applications and challenges. *Vehicular Communications*, *19*, 100179.
11. Kang, J., Lin, D., Jiang, W., & Bertino, E. (2018). Highly efficient randomized authentication in VANETs. *Pervasive and Mobile Computing, 44,* 31–44.
12. Shrestha, R., Bajracharya, R., Shrestha, A. P., & Nam, S. Y. (2019). A new type of blockchain for secure message exchange in VANET. *Digital Communications and Networks* **(in press)**.
13. Yang, Z., Yang, K., Lei, L., Zheng, K., & Leung, V. C. M. (2019). Blockchain-based decentralized trust management in vehicular networks. *IEEE Internet of Things Journal, 6*(2), 1495–1505.
14. Singh, M., & Kim, S. (2018). Branch based blockchain technology in intelligent vehicle. *Computer Networks, 145,* 219–231.
15. Bylykbashi, K., Elmazi, D., Matsuo, K., Ikeda, M., & Barolli, L. (2019). Effect of security and trustworthiness for a fuzzy cluster management system in VANETs. *Cognitive Systems Research, 55,* 153–163.
16. Cirne, P., Zúquete, A., & Sargento, S. (2018). TROPHY: Trustworthy VANET routing with group authentication keys. *Ad Hoc Networks, 71,* 45–67.
17. Zhao, J., Wu, Z., Wang, Y., & Ma, X. (2019). Adaptive optimization of QoS constraint transmission capacity of VANET. *Vehicular Communications, 17,* 1–9.
18. Debnath, A., Basumatary, H., Tarafdar, A., DebBarma, M. K., & Bhattacharyya, B. K. (2019). Center of mass and junction based data routing method to increase the QoS in VANET. *AEU -*

International Journal of Electronics and Communications, 108, 36–44.
19. Jadhav, P. P., & Joshi, S. D. (2019). WOADF: Whale optimization integrated adaptive dragonfly algorithm enabled with the TDD properties for model transformation. *International Journal of Computational Intelligence and Applications*, *18*(4), 1950026.
20. Revathi, K., & Krishnamoorthy, N. (2015). The performance analysis of swallow swarm optimization algorithm. In *Proceedings of the 2nd international conference on electronics and communication systems (ICECS)*.
21. Remmiya, R., & Abisha, C. (2018). Artifacts removal in EEG signal using a NARX model based CS learning algorithm. *Multimedia Research, 1*(1), 1–8.
22. Shrestha, R., Bajracharya, R., Shrestha, A. P., & Nam, S. Y. (2019). A new type of blockchain for secure message exchange in VANET. *Digital Communications and Networks*.
23. Lu, Z., Liu, W., Wang, Q., Qu, G., & Liu, Z. (2018). A privacy-preserving trust model based on blockchain for VANETs. *IEEE Access, 6,* 45655–45664.
24. He, Y., Yu, F. R., Wei, Z., & Leung, V. (2019). Trust management for secure cognitive radio vehicular ad hoc networks. *Ad Hoc Networks, 86,* 154–165.
25. Liang, J., Chen, J., Zhu, Y., & Yu, R. (2019). A novel intrusion detection system for vehicular ad hoc networks (VANETs) based on differences of traffic flow and position. *Applied Soft Computing, 75,* 712.
26. Ali, I., Gervais, M., Ahene, E., & Li, F. (2019). A blockchain-based certificateless public key signature scheme for vehicle-to-infrastructure communication in VANETs. *Journal of Systems Architecture*, *99*, 101636.
27. Hasrouny, H., Samhat, A. E., Bassil, C., & Laouiti, A. (2018). Trust model for secure group leader-based communications in VANET. *Wireless Networks*, *25*(8), 4639–4661.
28. Li, H., Pei, L., Liao, D., Sun, G., & Xu, D. (2019). Blockchain meets VANET: An architecture for identity and location privacy protection in VANET. *Peer-to-Peer Networking and Applications, 12*(5), 1178–1193.
29. Mohan, Y., Chee, S. S., Xin, D. K. P., & Foong, L. P. (2016). Artificial neural network for classification of depressive and normal in EEG. In *2016 IEEE EMBS conference on biomedical engineering and sciences (IECBES)*.
30. Masadeh, R., Mahafzah, B. A., & Sharieh, A. (2019). Sea Lion Optimization Algorithm. *(IJACSA) International Journal of Advanced Computer Science and Applications, 10*(5).
31. Mirjalili, S., & Lewis, A. (2016). The Whale Optimization Algorithm. *Advances in Engineering Software, 95,* 51–67.
32. Hsu, C.-C., Lin, S.-H., & Tai, W.-S. (2011). Apply extended self-organizing map to cluster and classify mixed-type data. *Neurocomputing, 74*(18), 3832–3842.
33. Tai, W.-S., & Hsu, C.-C. (2012). Growing self-organizing map with cross insert for mixed-type data clustering. *Applied Soft Computing, 12*(9), 2856–2866.
34. McCall, J. (2005). Genetic algorithms for modelling and optimisation. *Journal of Computational and Applied Mathematics, 184*(1), 205–222.
35. Jafari, M., & Chaleshtari, M. H. B. (2017). Using dragonfly algorithm for optimization of orthotropic infinite plates with a quasi-triangular cut-out. *European Journal of Mechanics A/Solids, 66,* 1–14.

Nisha Malik is a Ph.D. student in the Faculty of Engineering and Information Technology at the University of Technology Sydney, Australia. She completed her Masters in Mobile and Pervasive Computing from IGDTUW, India, and Bachelors in Engineering with distinction in Computer Science from Savitribai Phule Pune University, India. She has authored some of the influential publications in the field of vehicular networks and blockchain. She also received best paper award for two of her publications in IEEE consumer electronic magazine. Her research interests include vehicular networks, information security, cloud computing, and blockchain.

Priyadarsi Nanda obtained his Ph.D. in Computing Science from University of Technology Sydney, Australia, Master's degree in Computer and Telecommunication Engineering from University of Wollongong, Australia and Bachelor of Engineering with Distinction in Computer Engineering from Shivaji University, India. He is a Senior Lecturer at the University of Technology Sydney (UTS), Australia with more than 29 years of experience specialising in research and development in cybersecurity, IoT security, Internet Traffic Engineering, wireless sensor network security and many more related areas. His most significant work has been in the area of Intrusion detection and prevention systems (IDS/IPS) using image processing techniques, Sybil attack detection in IoT based applications, intelligent firewall design. He has authored more than 100 research articles including Transactions in Computers, Transactions in Parallel Processing and Distributed Systems (TPDS), Future Generations of Computer Systems (FGCS) as well as many ERA Tier A/A* conference articles. In 2017, his work in cyber security research has earned him and his team the prestigious Oman research council's national award for best research.

Xiangjian He received the Ph.D. degree in Computing Sciences from the University of Technology Sydney, Australia, in 1999. Since 1999, he has been with the University of Technology Sydney. He is currently a full professor and the director of the Computer Vision and Pattern Recognition Laboratory. His research interests are image processing, pattern recognition, computer vision and network security.

Ren Ping Liu is a Professor and Head of Discipline of Network and Cybersecurity in the School of Electrical and Data Engineering at University of Technology Sydney. He was a co-founder and CTO of Ultimo Digital Technologies—a Blockchain company. He was the founding Research Program Leader of the Digital Agrifood Technologies in Food Agility CRC, a government/research/industry initiative to empower Australia's food industry through digital transformation. Prior to that he was a Principal Scientist and Research Leader at CSIRO, where he led wireless networking research activities. He specialises in system design and modelling and has delivered networking and cybersecurity solutions to a number of government agencies and industry customers. His research interests include wireless networking, cybersecurity, and blockchain. Professor Liu was the founding chair of IEEE NSW VTS Chapter and a Senior Member of IEEE. He served as Technical Program Committee chairs, Organising Committee chairs, and delivered keynote speeches in a number of IEEE Conferences. Prof Liu was the winner of Australian Engineering Innovation Award and CSIRO Chairman's medal. He has over 200 research publications and has supervised over 30 Ph.D. students.