Sybil Attack with RSU Detection and Location Privacy in Urban VANETs- an Efficient EPORP Technique

Nitha C Velayudhan (✉ nithacse@gmail.com)
Noorul Islam Centre For Higher Education
Anitha A
Noorul Islam Centre For Higher Education
Mukesh Madanan
Dhofar University

Research Article

Keywords: security, SXOR operation, sybil attack, malicious node, urban VANET, Rumour routing technique, emperor penguin optimization

Posted Date: July 12th, 2021

DOI: https://doi.org/10.21203/rs.3.rs-680396/v1

Version of Record: A version of this preprint was published at Wireless Personal Communications on September 24th, 2021. See the published version at https://doi.org/10.1007/s11277-021-09102-x.

Sybil Attack with RSU Detection and Location privacy in Urban VANETs- an Efficient EPORP Technique

[1]*Nitha C Velayudhan, [2]Dr. A. Anitha, [3]Mukesh Madanan

[1]*Research Scholar, Department of Computer Science and Engineering,
Noorul Islam centre for Higher Education, TamilNadu, India.
nithacse@gmail.com

[2]Associate Professor, Department of Computer Science and Engineering,
Noorul Islam Centre for Higher Education, TamilNadu, India.

[3]Lecturer, Department of Computer Science and Engineering,
Dhofar University, Salalah, Oman.

Abstract: Nowadays, Vehicular ad hoc networks (VANETs) has received interest in the research because it is used to provide the information for drivers and passengers. In the urban VANET, security and safety is a main issue in recent days because of different kinds of attacks. From the attacks, Sybil attack can be considered as a very difficult for urban VANET networks. Hence, in this paper Emperor Penguin Optimization based Routing protocol (EPORP) is developed for detecting the Sybil attack as well as increasing the system performance. The main objective of the research is detecting the Sybil attack as well as improve the security in VANETS. The initial objective is achieved with the help of Rumour riding technique which detect the Sybil attack in the urban VANET. Similarly, the security of the system is achieved with the help of Split XOR (SXOR) operation. In the SXOR operation, the optimal key is generated with the assistance of Emperor Penguin Optimization (EPO). The proposed method is implemented in NS2 platform and performances are evaluated by metrics such as delay, throughput, delay, encryption time and decryption time. The proposed method is compared with existing methods such as Whale Optimization Algorithm (WOA), Particle Swarm Optimization (PSO) and Firefly Algorithm (FA) respectively. While analyzing the delivery ratio, the proposed method has 0.96sec and the WOA, PSO and FA is 0.94, 0.92 and 0.90 respectively. From the analysis, the proposed method has the high delivery ratio value compared with the WOA, PSO and FA methods. Similarly, the other parameters are analyzed and compared with the existing methods.

Keywords: *security, SXOR operation, sybil attack, malicious node, urban VANET, Rumour routing technique and emperor penguin optimization.*

1. Introduction

Vehicular Ad Hoc Networks (VANETs) have arisen as a spine of the up and coming age of Intelligent Transport Systems (ITSs) in the course of the most recent twenty years, prompting more secure and more effective thruways. VANET is significant for human existence as these people travel out and about. The traffic framework is excessively fine for drivers and travelers to utilize a non-security application [2]. Researchers from both scholarly world and industry are zeroing in on keen vehicle frameworks for completely self-sufficient driving, including associated vehicle innovation and self-driving vehicles. In VANETs, moving vehicles can speak with one another by methods for between vehicle interchanges just as by methods for RSU-to-vehicle correspondences with close by Road side units (RSUs) [1, 4]. Complex and dynamic information created by associated vehicles and framework are traded and prepared continuously in the ITS to permit a wide scope of administrations, for example, street driving conditions and improvement of wellbeing, traffic the board, contamination control and upkeep of vehicles. Associated vehicles are normally outfitted with on-board units (OBUs) that permit the Road Side Units (RSUs) [7, 8] to share basic traffic-related data. In ITS tasks, associated vehicles are getting progressively significant for improving their exhibition by beating the limitations of static foundations. Be that as it may, the serious level of Vehicle-to-Infrastructure (V2I) correspondences straightforwardness and availability delivers the whole transportation framework exceptionally helpless against different dangers focusing on information, administrations and choices [11]. As with most different organizations, it is basic not exclusively to ensure transport, yet additionally to guarantee data security. VANET security is a significant test in light of the fact that there are different sorts of assaults that undermine moving vehicle correspondences.

There are some specialized troubles in VANET, high portability, directing, powerful geography, loss of data through its remote connection, among others [3]. Organization security is truly powerless. During the transmission of data, significant security issues may happen. The connection might be undermined and additionally broken by various types of assaults and there are deformities or anomalies that are normal for the correspondence framework. Various security dangers are confronting VANETs, which may hinder the effectiveness of VANETs and even the insurance of life [9]. One of these dangers is assaults by Sybil, where a few created characters are expected by a noxious vehicle. Various VANET applications can be hurtful to Sybil assaults. Sybil attack is perhaps the most risky dangers as it penetrates the fundamental assumption of VANETs-based applications that all data acquired is correct and trusted [10]. To disperse bogus messages, Sybil aggressors can make a few bogus personalities. A covetous driver, for instance, may manufacture that various vehicles are cruising close by, making a fantasy of gridlock. Different vehicles would then choose an elective course and empty the eager driver from the path. Since the created vehicles are really heavily influenced by one malignant hub, other organization conventions can be additionally overseen by the malevolent hub [5]. It is foreseen that a vehicle dispatching a Sybil attack would get captured since all the copy messages will come from a similar area. In thick organizations, in any case, mistakes in confinement can prompt continuous bogus positives. All the more altogether, to mislead its neighbors about its bearings, a shrewd aggressor can utilize directional reception apparatuses [6]. To upgrade VANET security, security conventions, formalization of norms and different examination of assaults have been recommended, yet the region is as yet immense to investigate. In driving, the accessibility of on-board GPS has upset the route framework. Additionally, the new presentation of short-range radar and Lidar (Light identification and reach) has given the virtual eye the improvement of the encompassing vehicle map and the utilization of cutting edge driver help frameworks (ADAS) to moderate route issues and expected mishaps by giving a mishap mindfulness cautioning [12]. While progressed detecting innovation drives vehicles to associated vehicles and completely self-sufficient vehicles, potential assailants should be covered by vehicular correspondence [14].

Lately, Sybil's attack on VANET has gotten more important. The assailant can add malignant hubs with numerous characters. There are many traffic issues because of this, for example, wounds, crashes, and so on. This paper proposes the Emperor Penguin Optimization Based Routing Protocol to settle the issues in VANETs.

The rest of the documents are followed as below. In the section 2, the recent literature review analysis is presented and the section 3, the proposed methodology is presented. In the section 4 and 5 has results discussions and conclusion part is mentioned.

2. Literature Review

Many researchers are focused to detect the Sybil attack in VANETs. Some of the research is reviewed in this section.

The conceivable Power Control Models (PCM) for the dispatch of Sybil assaults on VANETs were examined by Yuan Yao *et al.* [16]. They presented two essential models of Sybil assaults and three modern models of Sybil assaults with or without complete force control. To discover strange varieties in the RSSI time arrangement, which were then used to characterize Sybil hubs utilizing a straight SVM classifier, they proposed a Power Control Identification Sybil Attack Detection (PCISAD) plot. Broad reenactments and genuine analyses show that with power the board, their proposed gadget can adequately manage Sybil assaults.

To play out a broadly accessible, lightweight and full-disseminated recognition for VANETs, Yuan Yao et al. [17] introduced the Sybil attack recognition strategy dependent on Received Signal Strength Indicator (RSSI), Voiceprint. Voiceprint receives RSSI time arrangement as the vehicular voice and analyzes the comparability between all arrangement acquired, not at all like most past RSSI-based strategies that measure the total area or relative distance as per RSSI esteems, or direct factual testing dependent on RSSI disseminations. Voiceprint doesn't depend on any predefined model for radio spread and performs free discovery without unified hub uphold. What's more, they upgraded Voiceprint by empowering it to perform Service Channel (SCH) location to abbreviate the hour of perception.

An Adaptive Neuro-Fuzzy Inference Method (ANFIS) was proposed by Boucif Amar *Bensaber et al.* [18] to get an expectation model of the VANET insurance index. Their strategy for research starts with network reproductions to secure an information base of attack events. At that point, the last was genuinely arranged and analyzed. Finally, they present their proposed security level model utilizing the MATLAB tool kit that permits the organization weakness to be determined in case of an assault.

Talal Halabi *et al.* [19] introduced the security game model that empowers the insurance component actualized in the ITS to streamline the designation of accessible attack recognition assets while considering blended attack methodologies, as per which the aggressor focuses on numerous RSUs in a circulated way. The helpfulness of the ITS was evaluated in the security game regarding discovery rate, harm to the assault, and the significance of the data sent by the RSUs. Their methodology will permit the ITS to alleviate and expand the flexibility of the effect of assaults. The discoveries show that their methodology diminishes the attack impact by at any rate 20% comparative with the one that detachedly designates safeguard assets to RSUs to the procedures of assailants.

The Cooperative Intelligent Transport Systems (C-ITS) have been created by Marwane Ayaida *et al.* [20] to improve traffic wellbeing and achieve a driving encounter unrest. They proposed a circulated approach permitting the utilization of the traffic stream guideline to recognize Sybil assaults. To distinguish a possible Sybil assault, the fundamental idea was that every vehicle should follow its area. This was finished by contrasting the genuine precise speed of the vehicle with the one estimated utilizing V2V interchanges with close by vehicles. Utilizing the traffic stream essential graph of the segment of the street where the vehicles were voyaging, the estimated speed was inferred. Some definite reproductions performed utilizing the notable NS3 network test system with the SUMO traffic test system approved this discovery calculation.

In the Intelligent Transportation System (ITS), Vehicular Ad Hoc Networks (VANETs) have broad execution potential, for example, traffic light, mishap counteraction and in-vehicle infotainment. Assurance, in any case, has consistently been a test for VANETs, which can make genuine mischief the ITS. By gathering and examining traffic information from Road Side Units (RSUs) and associated vehicles progressively, they permit different street wellbeing and effectiveness applications, for example, enhanced traffic the executives, crash shirking, and contamination control. These frameworks, in any case, are amazingly inclined to information debasement assaults that can genuinely hinder their dynamic abilities. Conventional attack location frameworks don't represent the refined and changing strategies of aggressors and disregard the security asset restrictions of the ITS.As the rival can spread bogus messages with numerous manufactured personalities to target various applications in the ITS, the Sybil attack is viewed as a genuine security danger to VANETs. Sybil's attack can prompt genuine fender benders. It is consequently critical to recognize assaults from Sybil from the earliest starting point of their event. Nonetheless, it is exceptionally hard to recognize Sybil's assaults on metropolitan vehicle networks [13].

Next, there are unknown vehicles. There are no certainty chains that interface asserted personalities with genuine vehicles. Second, the security of vehicles in areas is of incredible concern. Vehicle position information can be exceptionally private. A moving vehicle may have just couple of moments to collaborate with another vehicle that is now and then experienced because of the high portability of vehicles. In a particularly brief timeframe, it is hard to make certain reliability between vehicles that convey. This makes making a threatening personality simple for a malignant vehicle, however extremely hard for others to check. What's more, short vehicle discussions call for Sybil attack discovery on the web. In the event that a Sybil attack is identified after the attack has finished, the identification conspires fizzles. Discovery of Sybil hubs dependent on RSSI is an effective framework against Sybil assaults that utilizes area assessment, appropriation check or correlation of similitudes to characterize Sybil hubs. Be that as it may, if Sybil hubs perform power control to alter transmission controls deliberately, the RSSI esteems acquired will change appropriately, bringing about wrong restriction or diverse RSSI time arrangement of these Sybil hubs. Hence, by conventional RSSI-based methodologies, it is extremely hard to recognize Sybil hubs from ordinary hubs.

As a rule, the Sybil attack has been viewed as hurtful to the geography of the organization, network association, and use of data transfer capacity. The deterrent of steering and altering in democratic base frameworks are two significant issues brought about by Sybil elements. It is viewed as exceptionally hard to recognize Sybil assaults since vehicle security should be kept up and it is essential to try not to associate personality to a particular vehicle. Furthermore, because of their high portability attributes, the vehicles make some restricted memories a couple of moments to interface with different vehicles they experience. A few strategies for distinguishing this sort of attack [15] are recommended. Numerous strategies are ordered into three general instruments, including 1) an asset testing system that isn't important for the discovery of Sybil assaults in a vehicular climate. 2) An area check component that for the most part utilizes neighboring vehicle information or outside equipment to recognize a high-rate assault. These models will bring about disseminated handling, which will be all the more expensive to present and will likewise require more than one shrewd vehicle (OBU-prepared vehicles and sensors) out and about. The Sybil attack identification is moderated in the paper by the steering convention (EPORP) in light of Emperor Penguin Optimization. The principle point of the investigation is to perceive the Sybil attack just as to improve the insurance of VANETS. The framework's insurance is accomplished with the assistance of the Split XOR (SXOR) measure. The ideal key is made in the SXOR activity with the guide of Emperor Penguin Optimization (EPO). In the accompanying segment, the intensive survey of the proposed approach is introduced.

3. Proposed Sybil attack detection scheme

In recent years, VANETs have been considered as important research department for developing Intelligent Transportation System (ITS). This system should provide security and safety to passengers and drivers. Thus, security of VANETs can be considered as a very important problem because it affects the communication among the vehicle to infrastructure and vehicle to vehicle. In VANET, the security of the system completely degrades because of malicious attacks and its required to prevent and identify the security attacks [21]. Normally, the VANET operates the communication through the nodes which acts node as well as routers. The router conditions, it may be worked as malicious node means, the complete operation is corrupted. Hence, secure EPORP is designed to detection of sybil attack in VANET during RSU connected scenario. This proposed protocol is used to authenticate the nodes in VANET by secure operations of authentication and encryptions. The system model of VANET with proposed protocol to detect the sybil attack during RSU connected system is presented in figure 1.

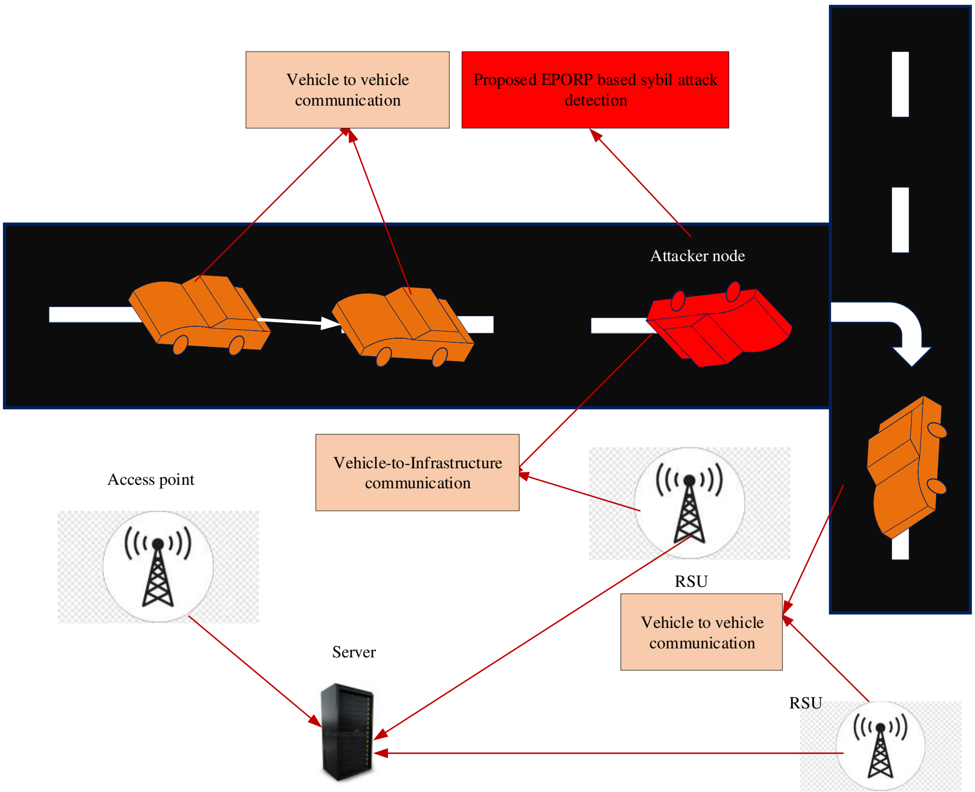

Vehicle to vehicle communication
Proposed EPORP based sybil attack detection
Attacker node
Access point
Vehicle-to-Infrastructure communication
RSU
Vehicle to vehicle communication
Server
RSU

Figure. 1 Block diagram of the proposed method

In the proposed methodology, the sybil attack is identified and secure the operation of VANET. Different types of attacks are available in VANET such as data flooding attack, selfish node attack, worm hole attack, jellyfish attack, modification attack and sybil attack. From these attacks, sybil attack is more harmful to VANET operation, so, it is considered in our work. From the figure 1, sybil attack, the VANET node have the many number identities are malicious nodes and additional identities are sybil node. The proposed sybil attack detection method should detect the malicious node also which prevent the malicious node operation with the help of sybil identities. Many different methods are available to detect the sybil attack such as position verification, identify registration and radio resource testing. However, these methods do not work perfectly in sybil attack detection. Hence, the proposed routing protocol with security constrains is used to detect the sybil attack in VANET. The attack surely affects the system physical integrity of the users. Hence, the confidentiality service also needed. To enhance the security, cryptographic methods are conventionally applied in communication networks. So, the VANET also, secure communication and quickly transmission is required in VANET. Thus, the proposed methodology is used to enhance the security and quick transmission by detect the sybil attack in VANET. The detail description of proposed routing protocol with security constraints is presented in following section.

3.1. Optimal Routing strategy to predict the sybil attack

The proposed routing protocol for VANETs, that provides the require route based on demands. In this protocol, the message is not sent normally, since the node receiver verify the number of secret keys will be transmitted to that node. The sender and receiver message also secured in the proposed protocol. The sender and receiver messages are secured with the help of SXOR operation. It is completely secure the message by encryption and decryption with specified generated key. The SXOR operation is presented in section 3.1.1. With the help of SXOR operation, the message of sender is secured which sent by encrypted form as well as key after authentication of receiver. The receiver can be authenticated with the help of Rumour riding process which contains the different kinds of questions. The questions are sent to the receiver, once receiver answered correctly, the required message as well as key is sent otherwise it is considered as sybil attacker or malicious node in VANET.

The Rumour riding process of authentication process is established. In the proposed optimal routing strategy, rumour riding process is used to find out the attacker node (Sybil attack). Once authentication is completed, the routing progress enabled in the proposed routing strategy. If a node required to start communication with another node means, initially, it authenticates with the help of Rumour riding procedure which described in section 3.1.2. After that, it sent route request message of RREQ to require communicate node.

The nodes by the individuals who need to pass this message register the data about the opposite route to the beginning node. A routing table is related with every node which consists the jump counter, lifetime, the emission identifier, the target sequence number, the sequence number source, the destination identifier and source identifier. After arriving at a node, the arrangement number (Destination Sequence Number) is verified if it's more prominent than the saved succession number to approve the path. At that point the node sends a RREP, with the data on the opposite path to the beginning node. When the route is set up, it is kept up by time, so as not to do all the packets and it stops at whatever point a packet shows up. On the off chance that a halfway node moves, geography changes so this node will not, at this point be utilized and the node quick foremost, from source to objective a blunder message on the route is communicated, RERR, the development of the node and subsequently the beginning node should begin again for the revelation of route inclusion. Finally, the process of proposed algorithm is presented below,

The proposed protocol operates with various steps. In the initial step, the message is encrypted with SXOR operation and transmitted to the neighbor node to know the status of neighbor node. After that, the node is authenticated with the help of Rumour riding procedure. The rumour riding procedure is utilized to identify the corrupted RSU which suddenly removed from the VANET. The sybil attack node as well as corrupted RSU is identified which collapse the system performance. Hence, the malicious RSU removed from the network during communication process. In the second step, the encrypted packet with the secret key is forwarded to all neighbor nodes in VANET. In the third step, the transmitted packet presence in the loop is validated. Finally, the neighbor node is safe, the secret key will be sent to that node. So, the packet request and packet response type are validated and packet is transmitted. In the proposed protocol, the sybil attack is detected with the use of tool command script and proposed protocol.

Phase 1: Start the connection

The main motive of the step is to fixed the components for starting the connection of new nodes which are need to connect the network. Before start the connection, the keys are generated using the EPO for SXOR operation. The keys are utilized to sign the routing tables sent among communication nodes. In the connection of nodes, the node should send the initial message with encryption. And, Rumour riding procedure is used to authentication procedure.

Phase 2: Computation of node reputation

The computation of reputation forms the basis of the model. The nodes should compute the reputation associated to neighbors' nodes [22]. This computation is operated with two sub phases.

- Calculation of the local reputation of the Node-Each Node will be able to calculate the reputation of its neighboring nodes locally. This is employed during the retransmission process of the message sent by the local node. The process includes messages not relayed by the node neighbor, malformed packets, unanswered requests, and delays in transmission.
- Calculation of the final reputation of the node

Phase 3: Nodes which forward broadcast messages during the RREQ selection

The selection of nodes that forward the RREQ packet continues to maintain the same concept for its determination. Based on the value of WILLING, and including a new factor to determine the selection, this factor will become the final reputation of the node, calculated according to the following algorithm.

Phase 4: Sending routing information

Routing tables can now be transmitted by the selected nodes. The selected node must sign the message routing using a private key, generated by the encryption algorithm. In this way, the selected node will be authenticated. As the next selected node is received by the routing table, it will be able to validate the identity of the node, based on the digital signature, which is already known beforehand. Additionally, the nodes must calculate the hash of the routing message to send, which will allow the nodes to validate the integrity of the message to run the same hashing algorithm used by the issuer, locally, and compare the submitted hash with the locally calculated hash.

3.1.1. Rumour riding procedure

The Rumour riding process has been developed to predict the corrupted RSU or attack node or malicious nodes in the VANET network. This protocol completely identifies the corrupted RSU in the VANET. Once, the corrupted RSU is identified with the help of Rumour riding procedure, the corrupted RSU is removed from the network for avoiding system collapse. The attacker may be on the identified initiator, intermediate, and responder nodes by using the rumour riding technique. The requested node sends a query to neighbours to gather the necessary resources. When the start-up node acts as a malicious node, it creates a fake request and launches fake search resources [23]. The selected node (neighbouring node) may act as a malicious node, which degrades the system performance. The responder node may act as a malicious node, which sends a duplicate response to the initiator node. The different attack conditions are illustrated in Figure 2, 3 and 4. The initial attack completely disrupts the system's performance, sending a duplicate response to the remaining node in the network of names as the request node. The attacker can be identified with the help of the rumour riding technique. Resources are encrypted and stored on each node. Here, cannot assign a key to the user to access resources without verifying node behaviour. The process presented in the rumour ride is verifiable through different queries. The resources and malicious nodes are identified with the different conditions of rumour riding operation. The detail descriptions of the proposed rumour riding is presented in this section.

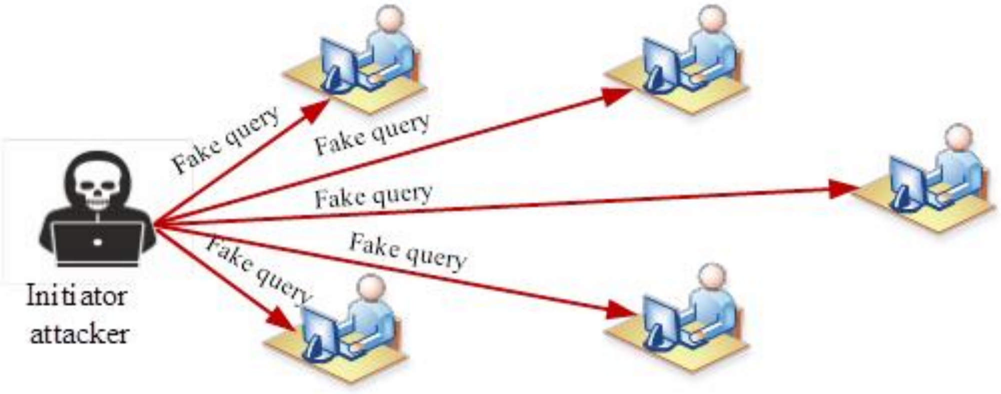


Figure. 2 Initiator or requester node attacker

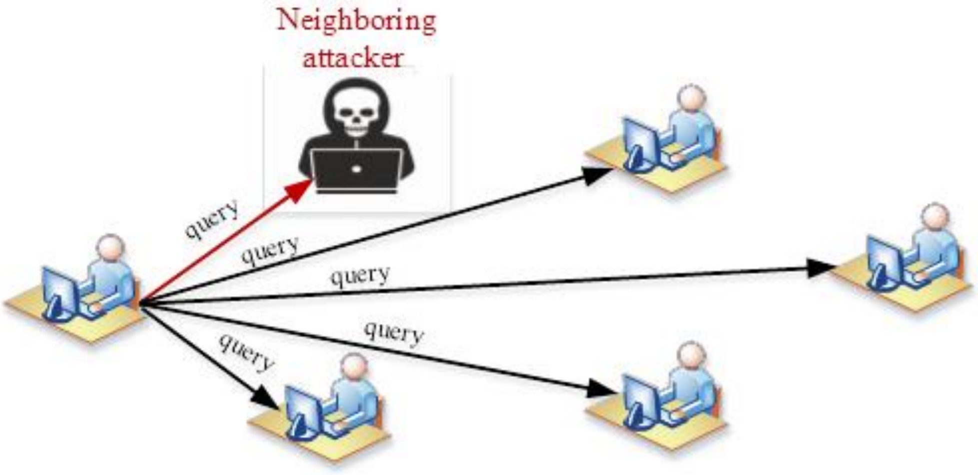


Figure. 3 Neighbouring or intermediate node attacker

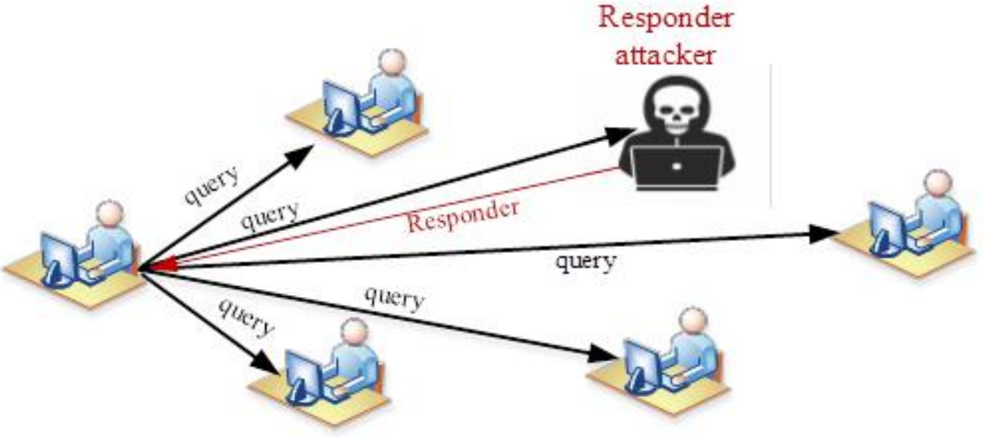


Figure. 4 Responder node attacker

From the VANET network, the attacker node can find with a challenging query in the rumour routing technique. The initiator node or requester node sends a query message with the listed challenge questions; what is IP address, what is the success rate and what is the location. Three queries are sent to neighbouring nodes with query. The attacker does not have the answers to those questions and secure node only knows the solutions. Depending on the situation, the status of each node can be obtained and the required resources are collected from the neighbour in the VANET network. The IP address, location, and success rate can be assigned based on earlier transactions to each node in the initial state, which will help identify the status of each node [24]. The rumour riding technique is used to identify the attacker node in VANET network which increases performance of system. The neighbour node is selected based on probability value which also considered as initial selection of node for compensating required resources. After that, selected node can be verified with rumour riding technique for identifying the attacker node or safe node scenario. Safe node or RSU means, immediately start the transaction progress in VANET network. If corrupted RSU is identify in VANET network, it suddenly removed from the network. To secure data resources in each node, SXOR is developed. The SXOR operation used to secure storage of resources in each node. The detail description of SXOR operation is described in below section.

3.1.2. SXOR operation

Additionally, the SXOR also introduced to secure data resources in each node by encryption when required resources to access which taken by decryption. The key also developed which only knows by data saver in nodes. In VANET network, each node has specified data resources which must be stored in secure manner. If not maintain in secure means, any unauthorized person will able to access the data resources in nodes. The secure storage is achieved with the utilization of SXOR operation [25]. The SXOR operation is an efficient secure operation which operated in modes of sent before nodes and retrieve data from nodes. The data resources are store in responder nodes before sent data resources to requester nodes. In the first mode of operation, sent before to requester nodes, data resources are securely stored with SXOR operation. The process of XOR operation can be illustrated in figure 5.

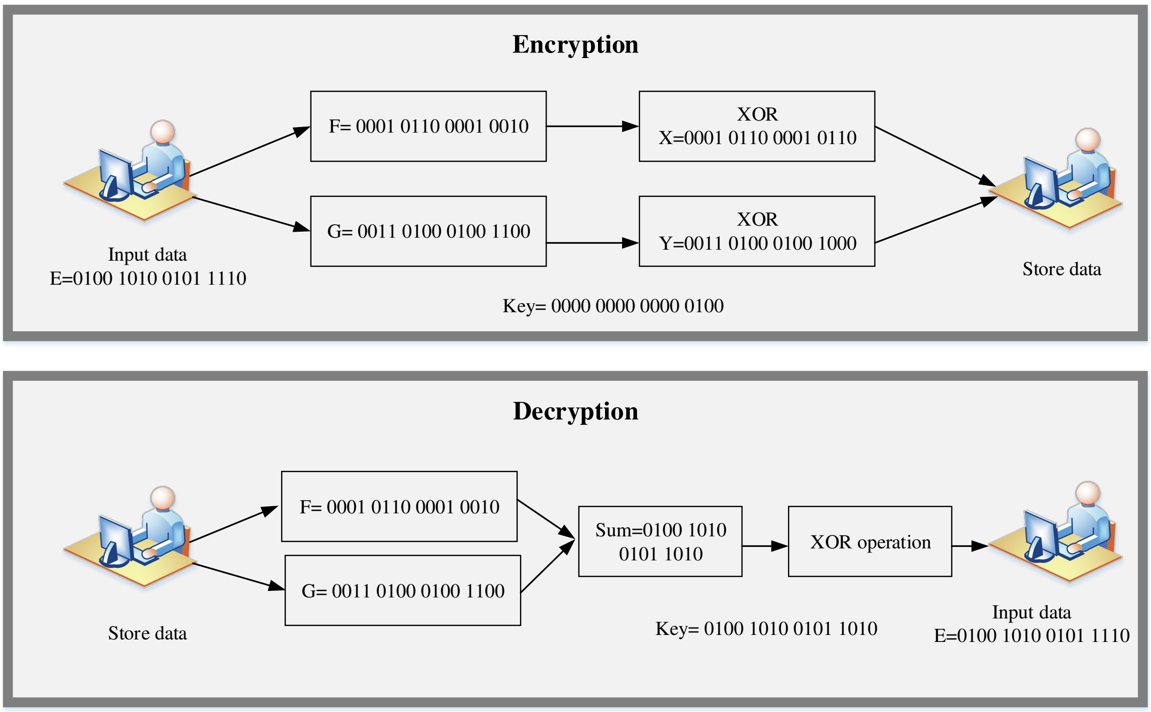


Figure. 5 Process of SXOR operation

The random key is used to generate the key rated as 0100 are used to perform XOR operation with the split elements of E and F which selected with the help of EPO algortihm. The XOR function can be obtained mathematically as follows,

$$X = F\ XOR\ key \tag{1}$$

$$Y = G \; XOR \; key \tag{2}$$

Where, X and Y values are $X = 0001\ 0110\ 0001\ 0110$ and $Y = 0011\ 0100\ 0100\ 1000$. On the split elements stored in the nodes, after performing the XOR operation. This split data can then be sent to colleagues with the key once the nodes status is checked. The SXOR function can split input resources into two parts, which cannot be achieved by abusers and attackers, effectively because it is impossible to predict the key value and data elements [26]. Data resources are obtained by the requestor, which attempts to retrieve the data through the encryption process. Some steps must be followed to retrieve data from the encryption process. First, the split data performs the XOR function with the key separately. From the SXOR function, achieve two different values such as $F = 0001\ 0110\ 0001\ 0010$ and$G = 0011\ 0100\ 0100\ 1100$. After that, these two values can be summed and $E = 0100\ 1010\ 0101\ 1010$. Send final data to do XOR function to achieve original input data. The final output of the encryption process is given mathematically as follows,

$$E = 0100\ 1010\ 0101\ 1110 \tag{3}$$

The SXOR function can store user data effectively. The key value is randomly generated and no split data carries any content information. The SXOR function, which provides high security, is used to store data resources on each node. Resources are managed securely in a VANET network with the help of SXOR operation. The SXOR operation also provides the location privacy of the users in VANETs. Many authors are designed the pseudonym changing approach for enabling the location privacy scheme. This scheme is processed to hide the real identify of the vehicles and also to decorrelate the identity of vehicles from their locations. The basic idea of this approach is as follows. Prior to joining the network, each vehicle must detain a set of pseudonyms that are changed regularly, so that the vehicle cannot be tracked by an adversary, and thus remains anonymous throughout the communication. But, in this proposed methodology, the vehicle identity also encrypted with the help of SXOR operation. So, the attacker not able to collect the original location of the vehicle with their identity. The original identity of the vehicle is optimally secured with the SXOR operation. The SXOR operation is utilized to secure the data as well as vehicle identify which enables the proper location privacy scheme in VANET. To select optimal key selection of SXOR operation, the EPO is used in proposed methodology. The detail description of EPO algorithm is presented below.

3.3. Process of Emperor Penguin Optimization

The EPO algorithm is developed based on the behavior of emperor penguin that scientifically named as Aptenodytes forsteri and it heaviest from the penguin species. From plumage and size, the female and male penguins are very much similar. The penguin has the black color dorsal side and head. Similarly, penguin have the white color belly, yellow color breast and bright yellow color patches. In the winter seasons, the emperor penguins spend their lives in open size in addition breeds. In the breeding periods, the penguins are coming ashore in large crowds that contains hundreds of thousands of penguins. The female penguin can be travel to 50 miles to reach ocean for getting prey even lay a single egg [27]. The hunting behavior and foraging behavior based, emperor penguin named as an animal in a group. Additionally, the emperor penguin have the ability to dive up to 1900 feet deeper and live below sea within 25 minutes. It can be stiffened and flattened wings with other penguin's species. To survive the Antarctic winter condition, the emperor penguins have the huddles. The huddling characteristics of emperor penguins are developed into four stages that presented below,

- Develop and compute the huddle boundary of emperor penguins
- Compute temperature profile surrounding the huddle
- Compute the distance among emperor penguins
- Emperor penguin can be relocating the effective mover

3.3.1. Mathematical modelling of EPO

The emperor penguins are working based on the huddling behavior that mathematical representation is presented in the section. The main objective of the emperor penguin is to find out effective mover of penguin. In the behavior, huddle is assumed to be presented on two different dimensional L-shape polygon plane. Initially, emperor penguins create the random huddle boundary. However, the temperature profile related the huddle can be computed. The distance among emperor penguins can also computed that will be useful for exploitation and exploration. At last, the effective mover is called as the best key generation which can be taken as the optimal key generation of SXOR operation. The best solution can be achieved and recalculate the huddle boundary conditions with updated positions of emperor penguins. The update positions of the process in the EPO is presented in the below section.

3.3.2. Create and compute huddle boundary

The emperor penguin generally updates the position themselves with the shape of polygon grid boundary under the huddling stage. In the huddling process, the emperor penguins have at least two neighbors that are selected randomly in the huddling procedure. In the huddle behavior, wind flow around huddle can be computed to find out the huddle boundary related a polygon. Moreover, the wind flow of the emperor penguin can be faster than the movement of a penguin. To described the randomly generated huddle boundary, concepts of complex variables in emperor penguin. The wind velocity α in addition, β can be defined as the gradient of$\emptyset$, which mathematically described in the below equation,

$$\beta = \nabla\emptyset \tag{4}$$

Where, δ can be mixed with $\emptyset$ to create the complex potential which can be described as the below equation,

$$S = \emptyset + j\delta \tag{5}$$

Where, S can be described as the analytical function and j can be described as the imaginary constant. The two dimensional environment of the emperor penguins is described in the equation (5). Generally, the penguins can be update their position randomly towards the position of emperor penguin that is to be presented as the centered of polygon region with L-shaped under highest effective fitness rate under iteration process.

3.3.3. Temperature profile regarding the huddle

Generally, the emperor penguins create huddle to increase the ambient temperature and conserve energy in the huddle. The situation can be mathematically modelled with the utilization of different assumptions that temperature is zero condition when radius of polygon can be less than one and temperature zero condition, the radius of polygon can be greater than one. Based on the exploration and exploitation procedure in the emperor penguins, the temperature profile is changed under different locations [28]. Under the huddle conditions, the temperature profile can be represented as below,

$$T_C = \left[T - \frac{MaX^{Iteration}}{Y - MaX^{Iteration}}\right] \tag{6}$$

$$T = \begin{cases} 0, & if\ P > 1 \\ 1 & if\ P < 1 \end{cases} \tag{7}$$

Where, T can be represented as time for computing best optimal results in search space, P can be represented as radius of polygon, Y can be represented as the present iteration and $MaX^{Iteration}$ can be represented as the maximum number of iterations.

3.3.4. Distance among emperor penguins

The distance among best attained optimal solution and emperor penguin can be computed after the creation of huddle boundary. When developed solution is close to the fitness solution that can be defined as the optimal solution. The remaining penguins (search agents) will update their positions related to current best optimal solution that are mathematically defined as follows,

$$\vec{d} = ABS\left(s(\vec{a}).\overrightarrow{r(Y)} - \vec{c}.\overrightarrow{r^s(Y)}\right) \tag{8}$$

Where, $\vec{a}$ and $\vec{c}$ can be coefficients that used for avoiding collision among neighbors, $\vec{d}$ can be represented as the distance among best fitness search agent and emperor penguin, $\overrightarrow{r^s}$ can be represented position vector of emperor penguins, $\vec{Y}$ can be represented as the current iteration, $\vec{r}$ can be represented as the best optimal pulses and $s(\vec{a})$ can be represented as the social forces of emperor penguins which is responsible to move towards the path of best optimal best solution that best search agents. The coefficient vectors are calculated based on the below equation,

$$\vec{a} = \left(m \times \left(T + r^{grid}\ (ACC)\right) \times Random\ ()\right) - T \tag{9}$$

$$r^{grid}\ (ACC) = ABS\left(\vec{r} - \overrightarrow{r^{s}}\right) \tag{10}$$

$$\vec{c} = Random\ () \tag{11}$$

Where, $Random\ ()$ can be represented as the random function lies in the range of [0, 1], $r^{grid}\ (ACC)$ can be represented as the polygon grid accuracy through comparing the difference among emperor penguins [29, 30], m can be represented as movement parameter that maintains a gap among search agents for avoid collision, parameter is set as the value 2, T can be represented as the temperature profile around the huddle. The function of the $s()$ can be computed in the below equation,

$$s(\vec{a}) = (\sqrt{F.e^{-\frac{y}{L}} - e^{-Y}})^2 \tag{12}$$

Where, F and L can be represented as control parameters for best exploitation and exploration that values the range of [2, 3]. The proposed EPO algorithm provides best results among these ranges.

3.3.5. Relocate the mover

The emperor penguin's positions are updated related to the best optimal solutions that is called as the mover. The changing position of the penguin is attained based on the mover responsible of different search agents in a presented search space and vacates the next position its presented position. The updating process of the next position of an emperor penguins are presented in the below equations,

$$\overrightarrow{r^{s}}(Y+1) = \overrightarrow{r(Y)} - \vec{a}.\vec{d} \tag{13}$$

Where, $\overrightarrow{r^{s}}(Y+1)$ can be represented as the next updated position of emperor penguin. In the iteration process, the penguin huddling characteristics is recomputed once the mover has been relocated. The final process of the EPO algorithm is presented below,

Step 1: Initialize the emperor penguin population, random key generation.

Step 2: Select the initial parameters, key generation and maximum iteration

Step 3: Compute the fitness value, in this proposed EPO algorithm random key generation are taken as the fitness function.

Step 4: Compute the huddle boundary conditions of the emperor penguin behaviors.

Step 5: Based on the huddle behavior, the temperature profile can be computed to attain the key generation of SXOR operation.

Step 6: Calculate the distance among the emperor penguins for update the positions of the penguins to select the best search agents.

Step 7: Based on the distance, the position of the penguins is updated.

Step 8: The boundary conditions of the emperor penguins.

Step 9: Compute the update search agent fitness value and update the position of lastly attained optimal key for SXOR operation.

Step 10: The algorithm is stopped when it reached the maximum iteration and optimal results are achieved.

Step 11: Finally, best optimal key of SXOR operation is find out which are feed to the encryption, it enhances the security of the VANET.

Finally, with the utilization of the proposed EPO algorithm, the optimal key generation of SXOR operation is computed based on the fitness function. The optimal key generation are able to enhance the security of the system. Additionally, the security is enabled with location privacy scheme in VANET. The performance of the proposed method is analyzed with the results section. The performance evaluation is essential to prove the efficiency of the proposed method. The simulation results of the proposed method is presented in the below section.

4. Performance analysis

The performance of the proposed method is analyzed with performance metrics. Based on the Sybil node attack detection and security control of proposed method, the performance of VANET network is developed under attacking condition. To prove the efficiency of the proposed method, it is analyzed with performance metrics such as delay, packet loss, delivery ratio, encryption time, decryption time and throughput. Delay can be defined as the time engaged aimed at a packet to be communicated diagonally the network from one node to another destination node. The proposed method is implemented in NS2 platform and results are analyzed. The implementation parameters of the proposed method are presented in table 1. The packet loss is derived as the disappointment of solitary or additional communicated packets to send the destination node from sender. The failure packet data can be considered as the packet loss. Delivery ratio can be derived as the percentage of packets gathered to the overall sending packet amount. Throughput is a measurement of how many units of packets can be processed in a given amount of time. The computation of performance metrics is presented in the given formula.

$$Delay = \frac{TD}{PR} = \frac{Total\ delivery\ time}{Packets\ received} \tag{14}$$

$$packet\ loss = Packet\ received(PR) - packet\ send(PS) \tag{15}$$

$$Delivery\ ratio\ DR = \frac{PR}{PS} \times 100\% = \frac{Packet\ ratio}{packet\ send} \times 100\% \tag{16}$$

$$Throughput = \frac{PR}{SE} \times SZ = \frac{Packet\ received}{Simulation\ end\ time} \times packet\ size \tag{17}$$

Based on the performance metrics, the verification and analysis of proposed method is done. The delay, packet loss of the proposed method should be in low which only considered as best performance system. The throughput and delivery ratio should be in high which only considered as best performance system. The proposed method is satisfying the above conditions related to performance metrics. The delay, packet loss, delivery ratio and throughput of the proposed method is simulated and illustrated in figure 6- 9.

Table. 1 Implementation parameters of the proposed method

S. No	Description	Parameters
1	Number of vehicles	150
2	Vehicle speed	12-30 m/s
3	Data generation	Poisson distribution
4	Packet Size	512 Bytes
5	Traffic constant	0.25
6	Road configuration	1 lane in each direction
7	Channel model	Nakagami m fading model
8	Signal to Noise ratio	20dB
9	Number of Access point	8
10	Simulation Area	1000m *1000m
11	Road length	5 km
12	Short time period	5 seconds
13	Road Side unit	10
14	Radio Range	300m

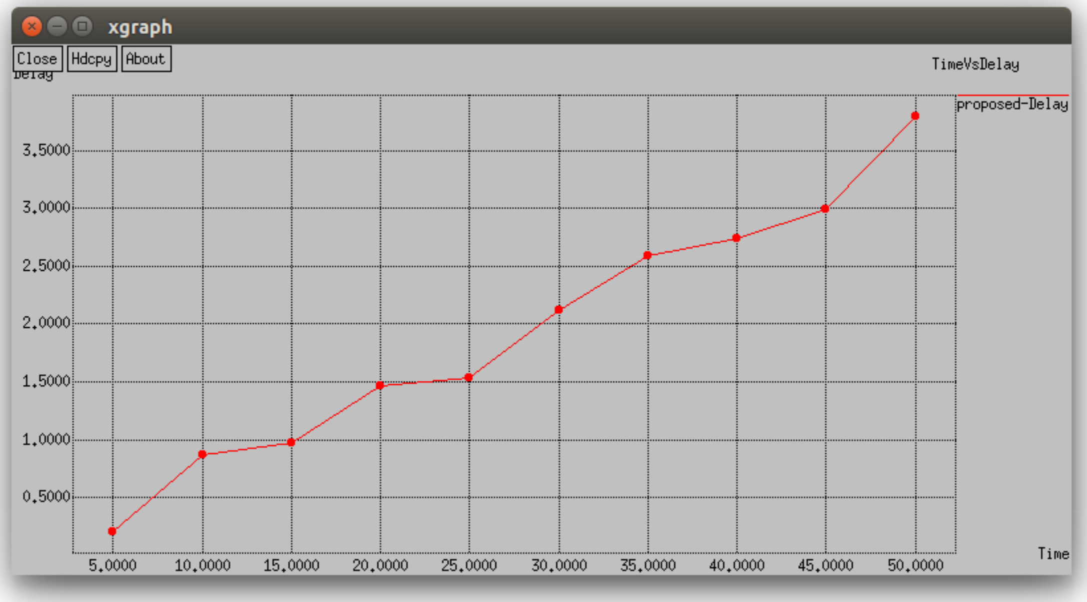


Figure. 6 Evaluation of Delay in proposed method

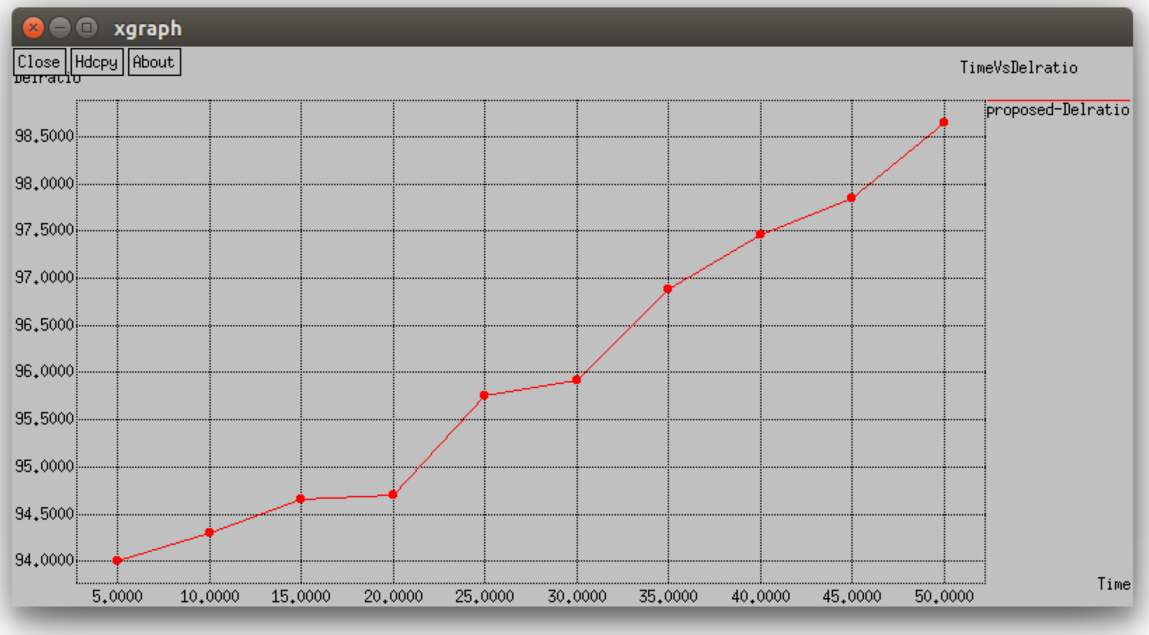


Figure. 7 Evaluation of Delivery ratio in proposed method

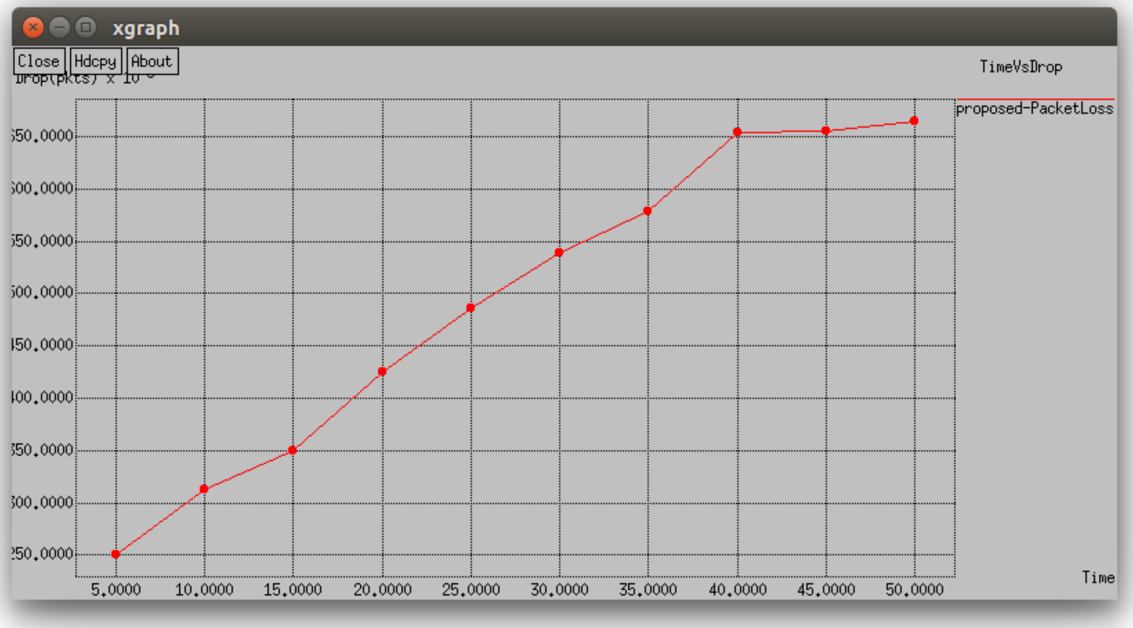


Figure. 8 Evaluation of Packet loss in proposed method

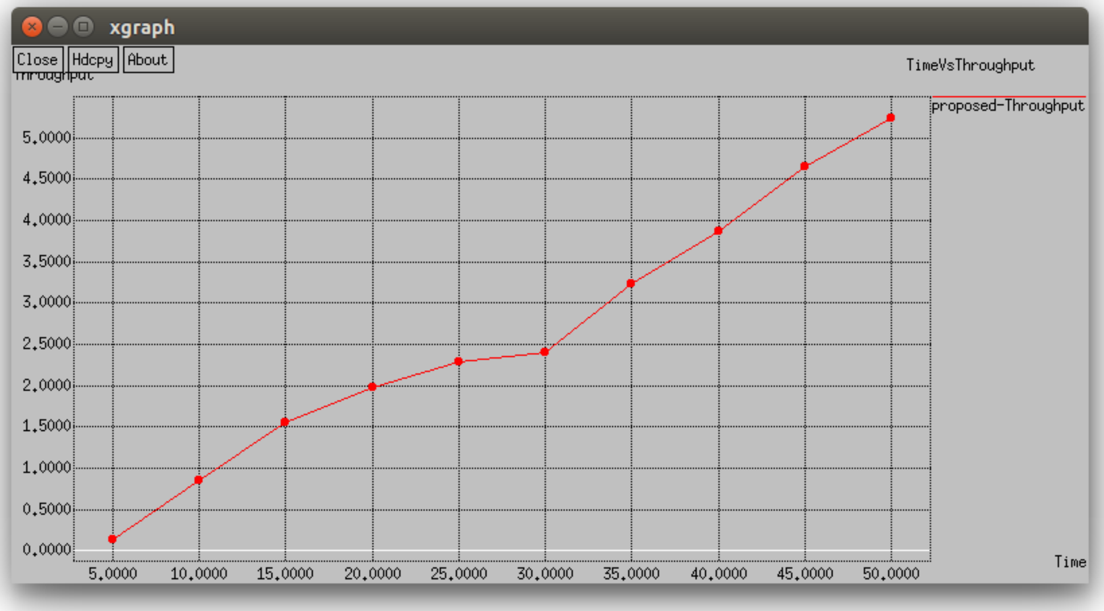


Figure. 9 Evaluation of Throughput in proposed method

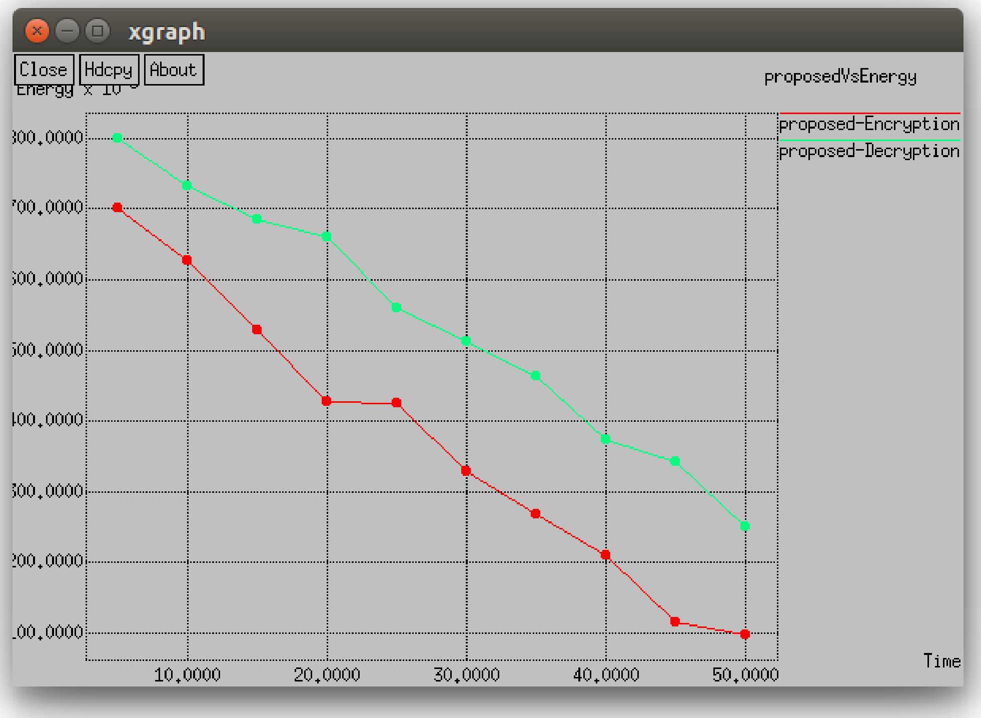
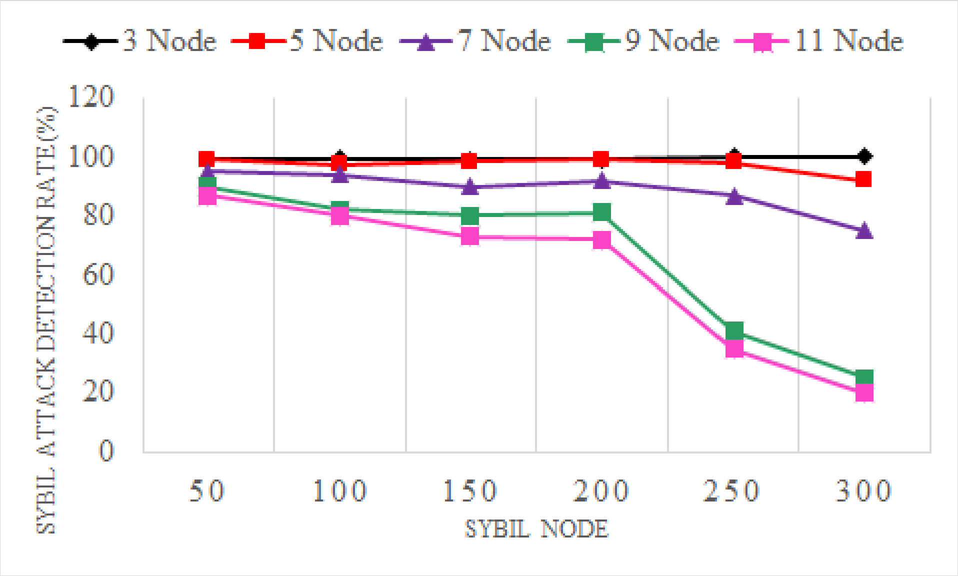
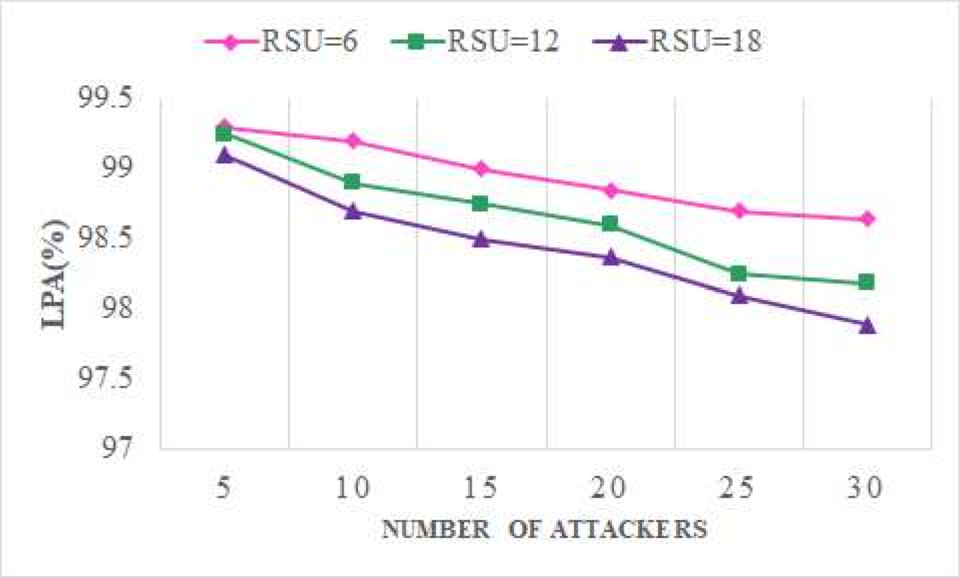


Figure. 10 Evaluation of Encryption and decryption time in proposed method



(a)



(b)

Figure. 11 Analysis of (a) Sybil attack detection rate and (b) Number of Attackers Vs LPA

A plot between the number of RSUs and the accuracy of location privacy for a different number of attackers is interpreted in Figure 11. If the number of RSUs in the same region increases, the interference range between RSUs increases as well, thus reducing the delay in certificate verification. The attackers are easily identified and eliminated by a large number of RSUs, and the accuracy of location privacy is enhanced. The proposed method achieves 98.54 percent LPA for 15 attackers in figure 11 of the maximum number of 18 RSUs in the 4x4 km^2 area.

The performance metric of delay is illustrated in figure 6 which must have attained in low value. The proposed method have the minimum delay value is 0.2×10^{-4} at 5ms. Similarly, maximum delay values are changed to 0.9×10^{-4} at 10ms. The delay value of proposed method is directly proportional to time domain values. The delay values are increasing based on time values increasing vice versa. The minimum limit of delay is 0.2×10^{-4} at 5ms and maximum limit of delay is 3.8×10^{-4} at 50ms. In the proposed method is implemented in 50ms only and results are analyzed. The performance metric of proposed delivery ratio is illustrated in figure 7 which must have attained in high value. The proposed delivery ratio minimum value is 94 at 5ms and maximum delivery ratio is 99.9 at 50ms. The performance metric of packet loss is illustrated in figure 8 which must have attained in low value. The proposed method has the packet loss value is 0.02 at 5ms. Similarly, packet loss values are changed to 0.031 at 10ms. The minimum limit of packet loss is 0.02 at 5ms and maximum limit of delay is 0.068 at 50ms. The performance metric of throughput is illustrated in figure 16 which must have attained in high value. The proposed method have the throughput value is 0.1×10^{10}at 5ms. Similarly, throughput values are changed to 0.8×10^{10} at 10ms. The minimum limit of throughput is 0.1×10^{10} at 5ms and maximum limit of throughput is 5.2×10^{10} at 50ms. The resources of each node in VANET network can be stored securely with the help of SXOR operation. The SXOR operation is working based on encryption and decryption methods. The specific time of encryption and decryption is presented in figure 9.

4.2. Comparison analysis

The comparison analysis is an essential part in research paper to prove efficiency of the proposed method. The proposed method of Sybil attack detection of VANETs networks is achieved with the help of EPO algorithm. The node can send query to other neighbouring node by request. The request is send to each neighbouring node which check them resources with request resources. From neighboring node which have same resources related to request resources that one ready to send requestor resources. The query sending and get resources in VANET networks consumes large waiting time. To reduce the waiting time, load balancing control and security enhancements, the proposed method is developed. The proposed method is compared with existing methods such as WOA, ACO and FA methods. The comparison analysis of proposed method is analyzed with performance metrics such as delay, delivery ratio, throughput and packet loss.

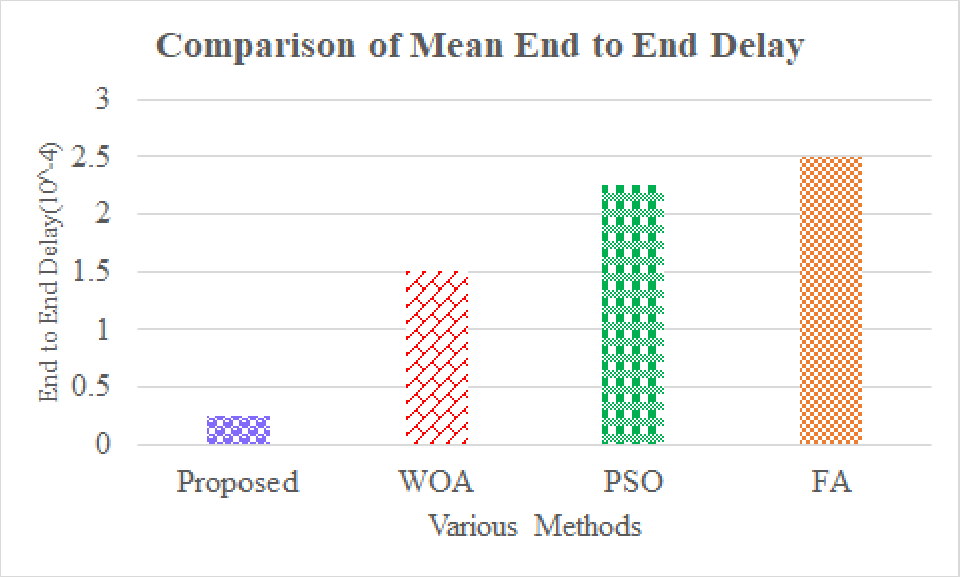


Figure. 12 Comparison of delay in proposed method

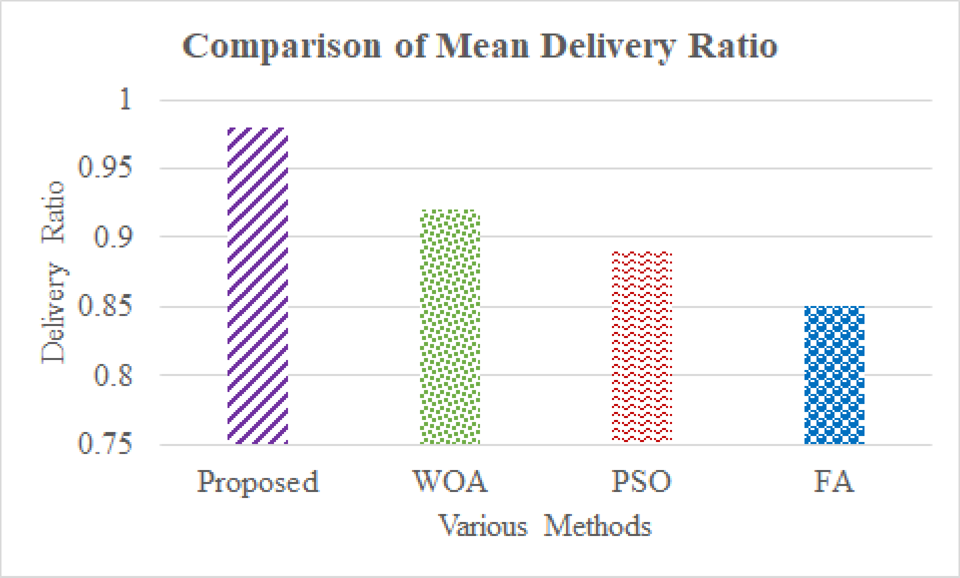


Figure. 13 Comparison of Delivery ratio in proposed method

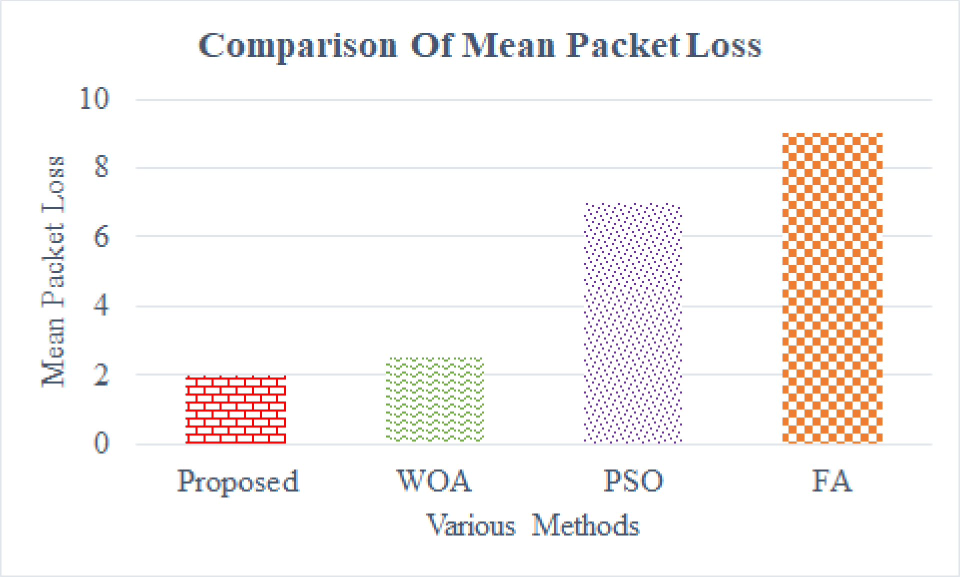


Figure. 14 Comparison of Packet loss in proposed method

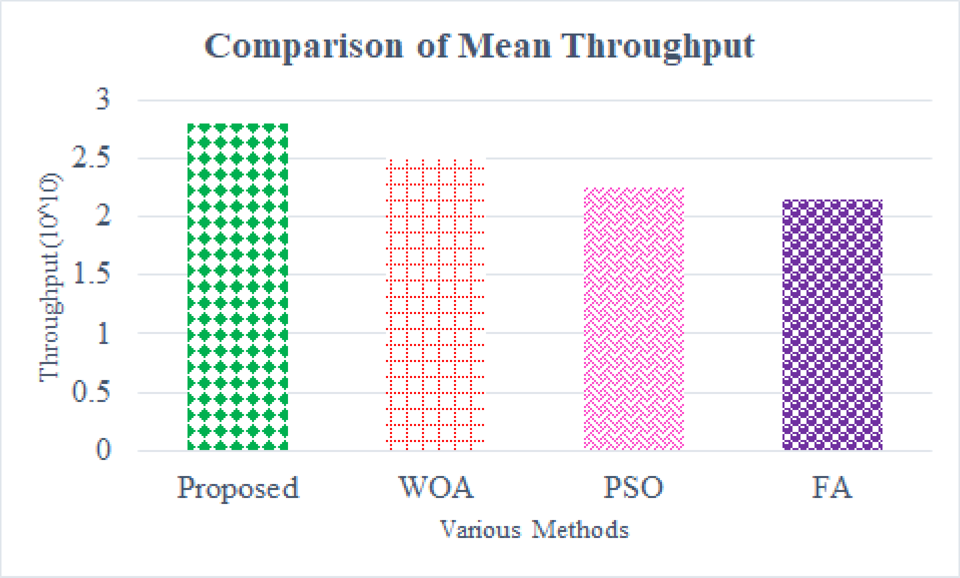
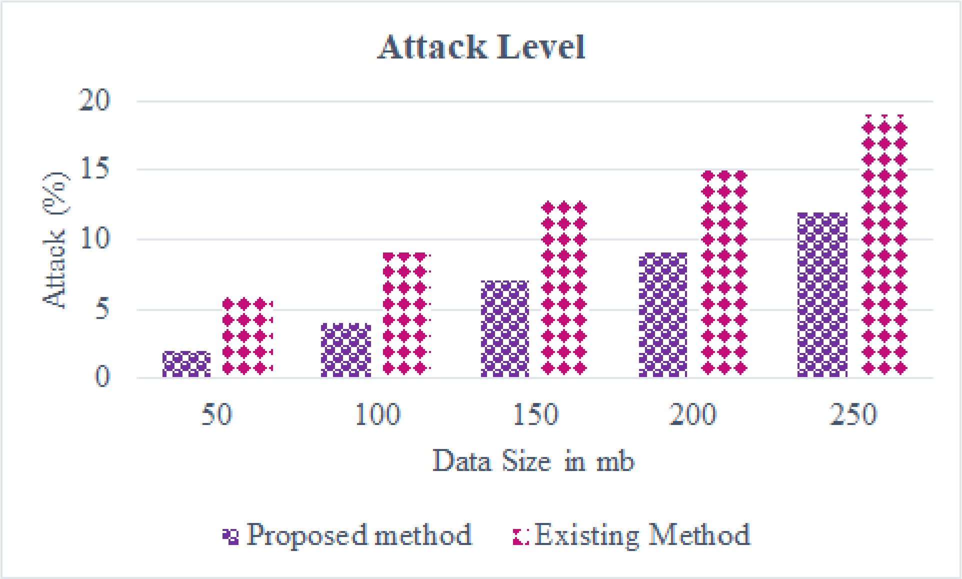
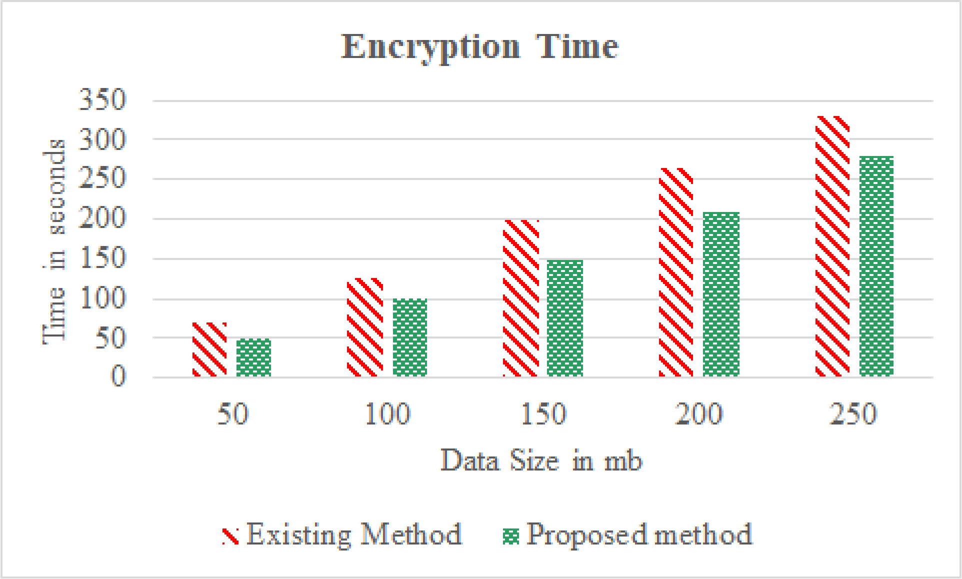


Figure. 15 Comparison of Throughput in proposed method

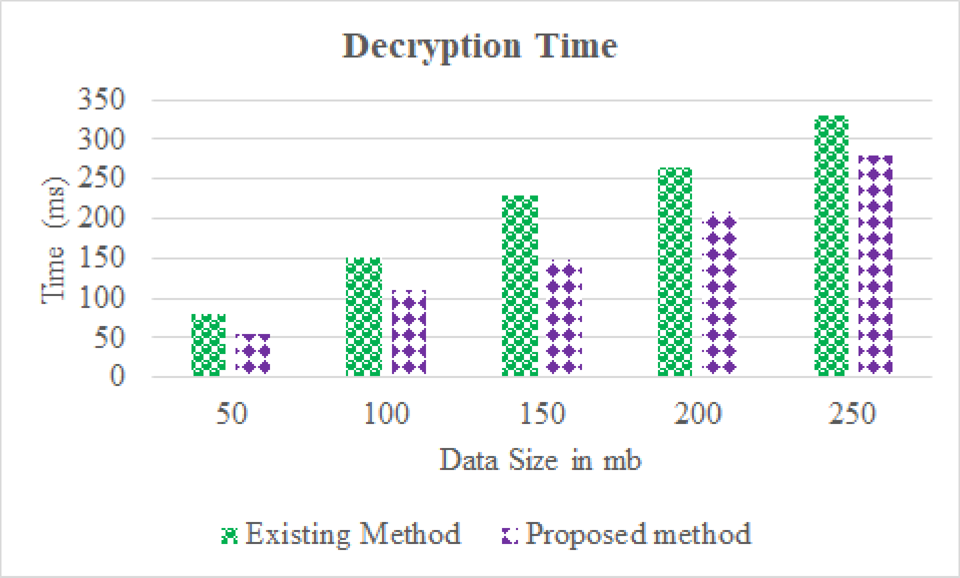
The comparison analysis of the proposed method performance metrics is illustrated figure 12-15. In the figure 14 describes the delay values of proposed and existing methods. From the figure, the proposed method have the delay values is 0.20×10^{-4}; the WOA have the delay values is 1.2×10^{-4}; the PSO have the delay values is 2.1×10^{-4}; the FA have the delay values is 2.6×10^{-4}. From the analysis, the proposed method has the low delay value compared with the WOA, PSO and FA methods. In the figure 13 describes the delivery ratio values of proposed and existing methods. From the figure, the proposed method has the delivery ratio values is 0.96; the WOA have the delay values is 0.94; the PSO have the delivery ratio values is 0.92; the FA have the delivery ratio is 0.90. From the analysis, the proposed method has the high delivery ratio value compared with the WOA, PSO and FA methods. In the figure 12 describes the packet loss values of proposed and existing methods. From the figure, the proposed method has the packet loss values is 1.97; the WOA have the packet loss values is 2; the PSO have the packet loss values is 7; the FA have the packet loss values are 9. From the analysis, the proposed method has the low packet loss value compared with the WOA, PSO and FA methods. In the figure 13 describes the throughput values of proposed and existing methods. From the figure, the proposed method have the throughput values2.6×10^{10}; the WOA have the throughput values is2.5×10^{10}; the PSO have the throughput values is2.3×10^{10}; the FA have the throughput values is2.1×10^{10}. From the analysis, the proposed method has the high throughput value compared with the WPA, PSO and FA methods. Based on the comparison analysis, we can conclude, the proposed technique is delivers the optimal solutions with efficiently.


Attack Level
Attack (%)
20
15
10
5
0
50
100
150
200
250
Data Size in mb
Proposed method
Existing Method

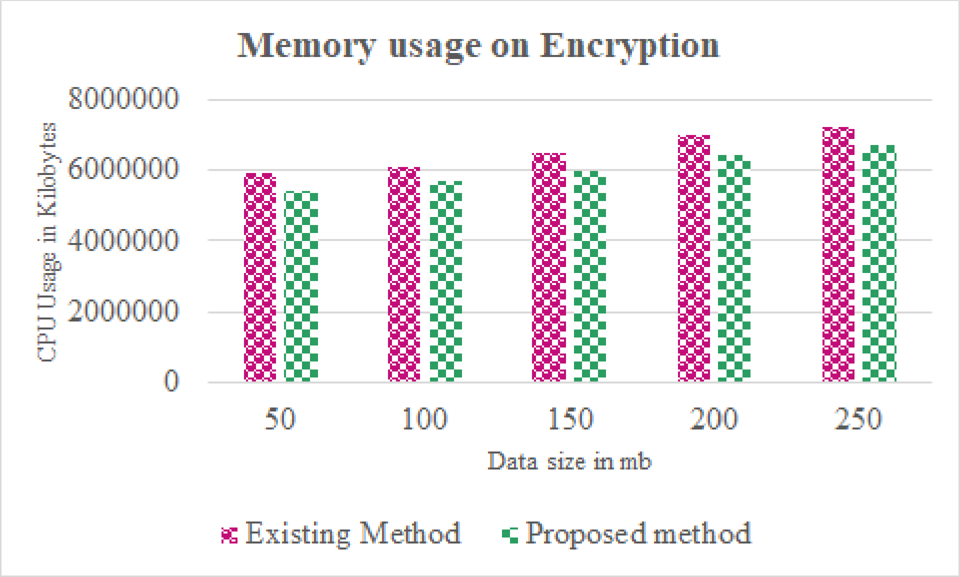
(a)


Encryption Time
Time in seconds
350
300
250
200
150
100
50
0
50
100
150
200
250
Data Size in mb
Existing Method
Proposed method

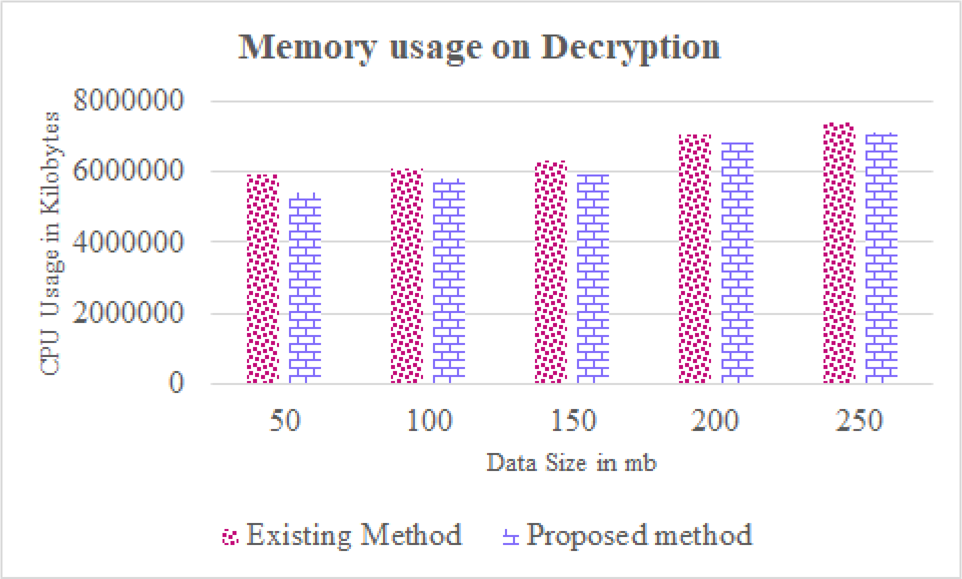
(b)


Decryption Time
Time (ms)
350
300
250
200
150
100
50
0
50
100
150
200
250
Data Size in mb
Existing Method
Proposed method

(c)

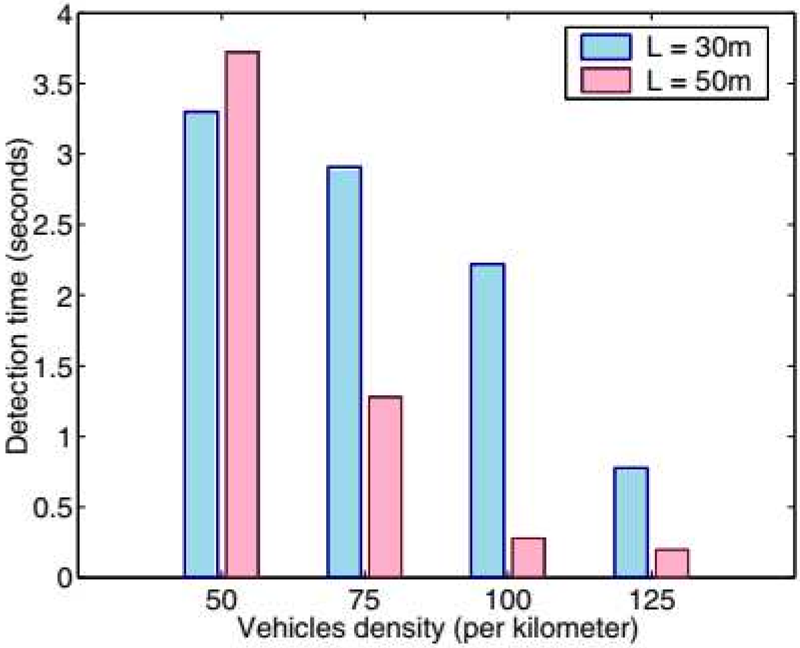

Memory usage on Encryption
CPU Usage in Kilobytes
8000000
6000000
4000000
2000000
0
50
100
150
200
250
Data size in mb
Existing Method
Proposed method

(d)

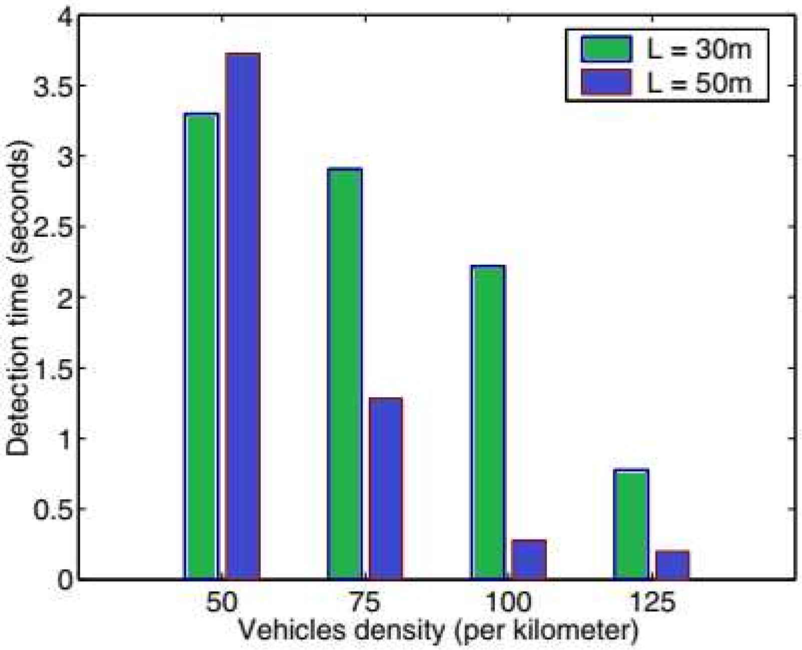


(e)

Figure. 16 Analysis of (a) attack level, (b) encryption time, (c) decryption time, (d) memory usage on encryption, (e) memory usage of decryption

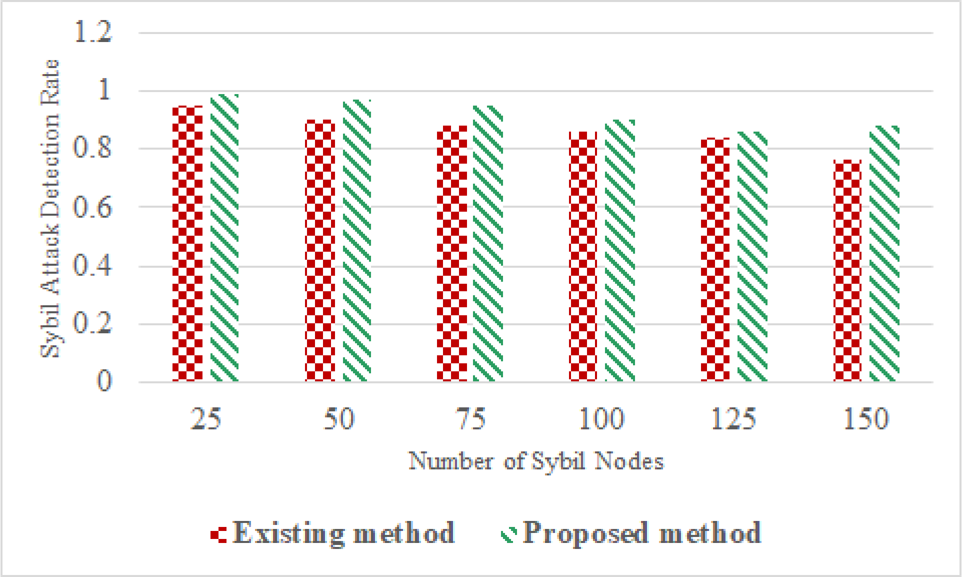


(a)

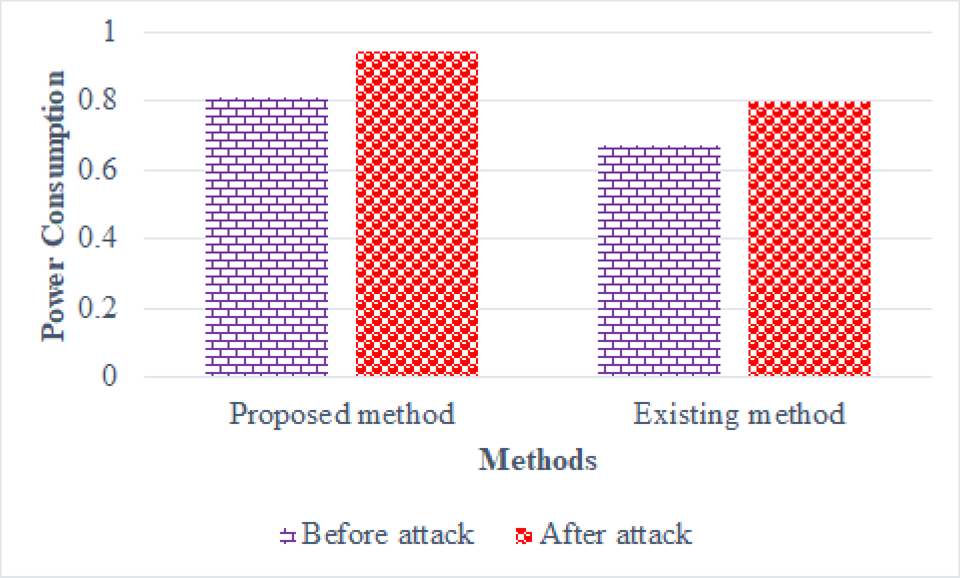


(b)

Figure. 17 Analysis of vehicle density in (a) various security levels and (b) various distances



(a)



(b)

Figure. 18 Analysis of (a) Sybil attack detection rate and (b) power consumption

The comparison analysis is an essential part in research paper to prove efficiency of the proposed method. The proposed method of security enhancement of VANET is achieved with the help of optimal routing algorithm. The comparison analysis of the proposed method performance metrics is illustrated figure 17. In the figure 17(a) describes the attack value of proposed and existing methods. From the figure (a), the proposed method has the attack values is 12%; the WOA have the attack values is 19%. From the analysis, the proposed method has the low attack value compared with the WOA methods. In the figure 17(b) describes the encryption time of proposed and existing methods. From the figure (b), the proposed method has the encryption time is 280 ms; the WOA have the encryption time is 320 ms. From the analysis, the proposed method has the low encryption time compared with the WOA methods. In the figure 17(c) describes the decryption time of proposed and existing methods. From the figure (c), the proposed method has the decryption time is 280 ms; the WOA have the decryption time is 320 ms. From the analysis, the proposed method has the low decryption time compared with the WOA methods. In the figure 17(d) describes the memory usage on encryption of proposed and existing methods. From the figure (d), the proposed method has the memory usage on encryption is 6000000kb; the WOA have the memory usage on encryption is 7000000kb. From the analysis, the proposed method has the low memory usage on encryption compared with the WOA methods. In the figure 14(e) describes the memory usage on decryption of proposed and existing methods. From the figure (e), the proposed method has the memory usage on decryption is 7100000kb; the WOA have the memory usage on encryption is 7500000kb. From the analysis, the proposed method has the low memory usage on decryption compared with the WOA methods. Figure 18 (a) and (b) shows the Sybil attack detection ratio and power consumption. Based on the analysis, the proposed method provides the best security and Sybil node detection in VANET network.

5. Conclusion

Sybil attack is main challenging attack in the VANETS. In this research, the EPORP based secure protocol is presented to detect Sybil attack and enhancing security of the system. The Sybil attack detection is a required task in VANET to reduce the system collapse condition. The Sybil attack is detected with the help of Rumour riding technique. Similarly, the message and information is secured with the help of SXOR operation. In the SXOR operation, the key generation is achieved with the help of EPO algorithm. So, the proposed methodology is enhancing the security as well as detect the Sybil attack in VANET. The proposed methodology performances were evaluated with the help of statistical measurements such as delay, throughput, encryption time and decryption time. The proposed method has been compared with the existing methods such as WOA< PSO and FA respectively. From the performance analysis and comparison analysis, the proposed methodology provides the best results related to enhance the security as well as system performance.

Data availability statements

Not applicable

Funding

Not applicable

Conflicts of interest/Competing interests

I have no conflict of interest.

Availability of data and material

Not applicable

Code availability

Not applicable

References

[1] Kiho Lim, Tariqul Islam, Hyunbum Kim and Jingon Joung, "A Sybil Attack Detection Scheme based on ADAS Sensors for Vehicular Networks", 2020 IEEE 17th Annual Consumer Communications and Networking Conference, CCNC 2020 (2020).

[2] Ilavendhan. A and Saruladha. K, “Comparative Analysis of Various Approaches for DoS attack Detection in VANETs”, Proceedings of the International Conference on Electronics and Sustainable Communication Systems, ICESC 2020 (2020) :821-825.

[3] O. Gietelink, J. Ploeg, B. De Schutter, and M. Verhaegen, “Development of advanced driver assistance systems with vehicle hardware-in-the-loop simulations,” Vehicle System Dynamics, (2006) 44(7):569-590.

[4] Kiho Lim, Kastuv M. Tuladhar and Hyunbum Kim, "Detecting Location Spoofing using ADAS sensors in VANETs", 2019 16th IEEE Annual Consumer Communications and Networking Conference, CCNC 2019 (2019).

[5] Bo Yu, Cheng-Zhong Xu, Bin Xiao, “Detecting Sybil attacks in VANETs”, Journal of Parallel and Distributed Computing, (2013) 73(6):746-756.

[6] Shan Chang, Yong Qi, Hongzi Zhu, Jizhong Zhao, and Xuemin (Sherman) Shen, “Footprint: Detecting Sybil Attacks in Urban Vehicular Networks”, IEEE Transactions on Parallel and Distributed Systems, (2012) 23(6):1103-1114.

[7] Fatih Sakiz and Sevil Sen, “A Survey of Attacks and Detection Mechanisms on Intelligent Transportation Systems: VANETs and IoV”, Ad Hoc Networks, (2017) 61:33-50.

[8] Nageswara Reddy Karukula, Sunar Mohammed Farooq, “A Route Map for Detecting Sybil Attacks In Urban Vehicular Networks”, Journal Of Information, Knowledge And Research In Computer Engineering, (2013) 2(2):540-544.

[9] Aleena Ann Jose, Alisha Pramod, Grace Philip, Deepika E.D and Sheba Jiju George, “Sybil Attack Detection in VANET Using Spider -Monkey Technique and ECC”, International Journal of Wireless Communications and Network Technologies, (2019) 8(3):31-34.

[10]

[11] D. Balamahalakshmi and K.N. Vimal Shankar, “Sybil Attack Detection with Reduced Bandwidth Overhead in Urban Vehicular Networks”, International Journal of Computer Science and Mobile Computing, (2014) 3(1):578-584.

[12] I.A. Sumra, H. Hasbullah, et al.,” VANET security research and development ecosystem, 2011 National Postgraduate Conference - Energy and Sustainability: Exploring the Innovative Minds, NPC 2011 (2011):1–4.

[13] H. Hasrouny, A.E. Samhat, C. Bassil, A. Laouiti, “VANET security challenges and solutions: a survey, Vehicular Communications, (2017) 7:7-20.

[14] Tong Zhou, Romit Roy Choudhury, Peng Ning, and Krishnendu Chakrabarty, “P2DAP – Sybil Attacks Detection in Vehicular Ad Hoc Networks”, IEEE Journal on Selected Areas in Communications. (2011) 29(3):582-594.

[15] Ali Pouyan and Mahdiyeh Parham – Alimohammadi, “An Effective Privacy-Aware Sybil Attack Detection Scheme for Secure Communication in Vehicular Ad Hoc Network”, Wireless Personal Communications, (2020) 113(2):1149-1182.

[16] Yuan Yao, Bin Xiao, Gang Yang, Yujiao Hu, Liang Wang, and Xingshe Zhou, “Power Control Identification: A Novel Sybil Attack Detection Scheme in VANETs using RSSI”, IEEE Journal on Selected Areas in Communications, (2019) 37(11):2588-2602.

[17] Yuan Yao, Bin Xiao, Gaofei Wu, Xue Liu, Zhiwen Yu, Kailong Zhang, and Xingshe Zhou, “Multi-channel based Sybil Attack Detection in Vehicular Ad Hoc Networks using RSSI”, IEEE Transactions on Mobile Computing, (2019) 18(2):362-375.

[18] Boucif Amar Bensaber, Caroly Gabriela Pereira Diaz, Youssef Lahrouni, “Design and modeling an Adaptive Neuro-Fuzzy Inference System (ANFIS) for the prediction of a security index in VANET”, Journal of Computational Science, (2020) 47:101234

[19] Talal Halabi, Omar Abdel Wahab and Mohammad Zulkernine, “A Game-Theoretic Approach for Distributed Attack Mitigation in Intelligent Transportation Systems”, Proceedings of IEEE/IFIP Network Operations and Management Symposium 2020: Management in the Age of Softwarization and Artificial Intelligence, NOMS 2020 (2020).

[20] Marwane Ayaida, Nadhir Messai, Geoffrey Wilhelm and Sameh Najeh, “A Novel Sybil Attack Detection Mechanism for C-ITS”, 2019 15th International Wireless Communications and Mobile Computing Conference, IWCMC 2019, (2019) :913-918.

[21] Mohamed Baza, Mahmoud Nabil, Mohamed Mohamed Elsalih Abdelsalam Mahmoud, Niclas Bewermeier, Kemal Fidan, Waleed Alasmary, and Mohamed Abdallah, "Detecting sybil attacks using proofs of work and location in vanets", IEEE Transactions on Dependable and Secure Computing (2020).

[22] Ankit Kumar, Vijayakumar Varadarajan, Abhishek Kumar, Pankaj Dadheech, Surendra Singh Choudhary, VD Ambeth Kumar, B. K. Panigrahi, and Kalyana C. Veluvolu, "Black hole attack detection in vehicular ad-hoc network using secure AODV routing algorithm", Microprocessors and Microsystems, (2021) 80:103352.

[23] Mary Subaja, Christo, and S. Meenakshi, "Reliable and Authenticated Rumor Riding Protocol for Unstructured Peer-to-Peer Network", Indian Journal of Science and Technology, (2016) 9(21):1-9.

[24] Mary Subaja, Christo and S. Meenakshi, "Enhancing Rumor Riding protocol in P2P network with Cryptographic puzzle through challenge question method", Computers and Electrical Engineering, (2018) 65:122-138.

[25] V.Siddaramappa, and K. B. Ramesh, "DNA-Based XOR operation (DNAX) for data security using DNA as a storage medium", Integrated Intelligent Computing, Communication and Security, (2019) :343-351.

[26] Yibin Li, Keke Gai, Longfei Qiu, Meikang Qiu, and Hui Zhao, "Intelligent cryptography approach for secure distributed big data storage in cloud computing", Information Sciences, (2017) 387:103-115.

[27] Sasan Harifi, Madjid Khalilian, Javad Mohammadzadeh, and Sadoullah Ebrahimnejad, "Emperor Penguins Colony: a new metaheuristic algorithm for optimization", Evolutionary Intelligence, (2019) 12(2):211-226.

[28] Sasan Harifi, Madjid Khalilian, Javad Mohammadzadeh, and Sadoullah Ebrahimnejad, "Optimization in solving inventory control problem using nature inspired Emperor Penguins Colony algorithm", Journal of Intelligent Manufacturing, (2021) 32(5):1361-1375.

[29] Harsimran Kaur, Anurag Rai, Sarvjit Singh Bhatia, and Gaurav Dhiman, "MOEPO: A novel Multi-objective Emperor Penguin Optimizer for global optimization: Special application in ranking of cloud service providers", Engineering Applications of Artificial Intelligence, (2020) 96:104008.

[30] Zhikai Xing, "An improved emperor penguin optimization based multilevel thresholding for color image segmentation", Knowledge-Based Systems, (2020) 194:105570.