ARPVP: Attack Resilient Position-Based VANET Protocol Using Ant Colony Optimization

Jyoti Maranur (jyotimaranur11@gmail.com)
Godutai Engineering College for Women
Basavaraj Mathapati
Appa Institute of Engineering and Technology

Research Article

Keywords: Ant colony optimization, attack resilient, position-based routing, self-trust model, reliable data transmission, vehicular ad-hoc networks.

Posted Date: August 2nd, 2021

DOI: https://doi.org/10.21203/rs.3.rs-718374/v1

ARPVP: Attack Resilient Position-based VANET Protocol using Ant Colony Optimization

Jyoti R. Maranur*, Asst. Prof. Computer Science and Engineering, Godutai Engineering College for Women, Kalaburagi, India, jyotirmaug16@gmail.com

Dr. Basavaraj Mathapati, Computer Science and Engineering, Appa Institute of Engineering and Technology, Kalaburagi, India, drbasu2014@gmail.com

Abstract. The position-based routing of Vehicular Ad hoc Network (VANET) vulnerable to various security attacks because of dependency on computing, control, and communication technologies. The Internet of Things (IoT)-enabled VANET application leads to the challenges such as integrity, access control, availability, privacy protection, non-repudiation, and confidentiality. Several security solutions have been introduced for two decades in two categories as cryptography-based and trust-based. Due to the high computation complexity, cryptography-based solutions are outperformed by recent intelligent trust-based mechanisms. The trust-based techniques are lightweight and effective against the well-known security threats in VANET. The objective of this paper has to design a novel position-based routing in which the conduct of vehicles assessed to accomplish reliable VANET communications. Attack Resilient Position-based VANET Protocol (ARPVP) proposed to detect and prevent malicious vehicles in the network using the trust evaluation technique and artificial intelligence (AI). In the first phase of ARPVP, the periodic self-trust assessment algorithm has designed using various trust parameters to detect unreliable vehicles in the network. In the second phase of ARPVP, the position-based route formation algorithm has designed using the AI technique Ant Colony Optimization (ACO). ACO solves the problem of reliable route formation by neglecting the attacker's using a trust-based fitness function. The trust parameters of each vehicle as mobility, buffer occupancy, and link quality parameters had measured in both phases of ARPVP. Simulation outcomes of the proposed model outperformed state-of-art protocols in terms of average throughput, communication delay, overhead, and Packet Delivery Ratio (PDR).

Keywords: Ant colony optimization, attack resilient, position-based routing, self-trust model, reliable data transmission, vehicular ad-hoc networks.

1 Introduction

Recently automotive manufacturing has been proven as one of the fastest rising industries due to rapid advancement in technology, especially the wireless communications among the vehicles enabled by the Internet of Things (IoT). The IoT-enabled VANET is a collection of vehicles and infrastructure devices like Road Side Units (RSUs) connected through the Internet [1]. The IoT has more than the most recent pair of a long time, become an issue in the insightful world, and transversely over different ventures. While getting logically unavoidable, IoT supports a thorough depiction of the state of being and not all that terrible degree of relationship with the actual world [2]. Zones, for instance, collaborations, Intelligent Transportation Systems (ITS), business/measure the heads, and e-prosperity are several instances of conceivable application fields where this novel point of view will be significantly important. The certification of IoT tremendously depends on various rules, for instance, the routing's design, networks, and interchanges, data dealing with, and inescapable figuring developments that help profitable, strong, and physical and computerized interconnectivity. A significant fundamental driving force of IoT that empowers the interconnection of plans is arranging, and unequivocally, guiding the framework. It incorporates the creation of traffic courses and communicating the directed paths from the source to the last destination in a framework. With billions of things interconnected in the framework, an extreme test confirming that the framework from various sorts of perils and attacks. Customers will feel unreliable about their data if they are powerless against attacks from unapproved individuals or machines over the framework.

Accordingly, security is by an expansive edge may be the best test in IoT networks [3]. A huge part of the security threats is performing at the routing layer, which suggests all through the data transmission method, in this way the keeping an eye on strong insurance from such perils will depend upon the security framework organized in routing helpfulness. Nonetheless, the cross-layer attacks additionally expanding these days to upset the correspondence networks to a huge broadening. Accordingly, making the strategy of secure interchanges in IoT is significantly also testing. This central prerequisite for

confirming the routing method flanked by an assortment of IoT gadgets over various heterogeneous networks needs exploration responsibilities [4] [5]. To reduce the troubles of secure routing in IoT engaged networks, different courses of action arranged at the routing layer from the latest decade. The security plans expected to recognize and ease the online protection risk, for instance, botnets, Denial-of-Service (DoS), malware, Distributed Denial-of-Service (DDoS), Man-In-Middle (MIM) attacks, sticking attacks, and so on. All such attacks are performed inside the network with the wrong intentions. To mitigate such attacks, not only strong measures are required but also minimum computation efforts for guaranteed network QoS. The cryptography-based methods introduced [6-13] for secure end-to-end data transmission, but these methods yet to address the challenges of key generation, encryption, and decryption processes with minimum computation overhead and higher security against the various threats. To overcome the problems related to cryptography-based techniques, recently the trust-based mechanisms gained significant attention.

Apart from the challenges of VANETs like highly dynamic network topology, load balancing, and fault tolerance, the nodes reliability analysis is also a vital factor. The unreliable vehicles need to be mitigated and select the reliable nodes for the transmission of data. In VANET, vehicles can communicate mistaken data both inadvertently, for example in case of a sensor disappointment, and purposefully when an attacker rolls out unapproved improvements to the product and equipment parts of the vehicle. These dangers are called figment attacks [14]. The counterfeit data broadcasting suggests that different participants change their course, mobility, and plan further activities based on the data received. It can be utilized by an attacker both to falsely diminish the gridlocks on his course and purposely produce an auto collision. Conventional routing strategies and data trustworthiness affirmation in remote networks are not compelling against such attacks just as having extreme calculation trouble [15]. As an approach to counter attacks focused on relevant data uprightness, the components based on notoriety and trust can be utilized when each network part has its degree of notoriety in the framework, and based on this level, the remainder of the participants conclude whether to trust the data got from this part. Nowadays the IoT applications [16-19] need reliability methods to protect from various security threats.

As the trust and reputation-based methods effective with minimum computation efforts, we proposed a novel secure position-based VANET routing protocol. The Attack Resilient Position-based VANET Protocol (ARPVP) is proposed to identify the attackers through weight-based trust calculations followed by AI-based stable and reliable route discovery. The novelty of the ARPVP protocol lies in the optimized position-based routing convention that evaluates vehicles to accomplish reliable VANET correspondences. The reliability achieved using the self-trust evaluation model. In the primary stage, the unreliable nodes recognition is detected, and in the subsequent stage, the reliable paths discovered using ACO for data transmission. Section 2 presents a survey of recent trust-based strategies for VANET. Section 3 presents the system of the proposed convention. Section 4 presents the reproduction results. Section 5 presents the end and future headings.

2 Related Works

Several methods proposed so far for reliability analysis and security in VANET communication using a trust-based approach. Some recent works are reviewed during this section. In a unique VANETs climate, there is a lot of vulnerability in concluding who to trust. Existing trust models in VANETs incorporate substance-arranged trust models and data-situated trust models. Element-arranged trust models center around the modeling of the trustworthiness of companions. Data-arranged trust models put more accentuation on assessing the trustworthiness of data.

A. State of Art

The author analyzed two kinds of conventions for secure routing in [20] for VANETs such as geography-based and position-based routings. Geography-based methods are customary ones for Mobile Adhoc Networks (MANETs); they utilize a source to objective data that put away in the routing table. The routing table in proactive conventions refreshes habitually on powerful geography, and they pick the most limited way calculation for routing. Receptive routing was utilized for large networks as they propose high portability and dynamic nature. At the point when the source speaks with the objective hub, the course was found continuously. Afterward, the sink node sends an acknowledgment message to the source. The half-breed method (Zone Routing) represents a mix of the initial two sorts and it is utilized by the network situation. The similitude-based trust and notoriety structure for VANETs was

proposed in [21]. The message must be checked in the wake of getting it. A similitude mining calculation was utilized to process the likeness between non-direct comparative data. Suggestions of operators and direct insight of the outcome were coordinated as notoriety assessments. When the message content was checked, the estimations of trust and notoriety are refreshed. Another calculation utilized for trust the executives proposed and named BARS (Blockchain-based Anonymous reputation System) in [22]. Vehicles utilize two blockchain instruments for verification based on evidence of essence and nonattendance. Public keys were utilized as pen names to secure vehicle protection. The communicated messages were recorded in one blockchain to assess the standing of vehicles. The outcomes have shown that BARS adequately improved the trustworthiness of communicated messages and ensures vehicle security effectively. The LSOT (Lightweight Self-Sorted out Trust) system was proposed in [23] as a calculation to secure VANETs interchanges. In the model, the nodes are self-composed; the total trust declaration based and proposal based execution. The ART (Attack-Resistant Trust) model proposed in [24] assessing the trustworthiness of both traffic data and vehicle nodes for VANETs as two separate measurements, specific data trust, and hub trust. Data trust was utilized to check data, yet the hub trust shows how trustworthy the nodes in VANETs are. To assess the proficiency of the proposed model, tests were conducted. The outcomes demonstrate that the Craftsmanship model adapts to pernicious attacks. The author utilized three markers for trust and proposed the trust assessment model based on boundaries of notoriety, experience, and information in [25]. Notoriety shows how well the trustee has traded data with the entirety of the substances up to this point. Experience demonstrates that how well the trustor has achieved trading data with the trustee as of recently. Information renders perception on the trustee (the vehicle which is giving data) as immediate trust. The detailed proof-hypothetical of the trust and notoriety model for VANETs with an augmentation of the normal derivation analytics (un)secured was introduced in [26] [27]. Utilizing a calculation, they could qualify the activity passed as a protected message through quite a few vehicles by checking at every cooperation that consistency is saved. Hence, the standing model is based on an assessment of defined input messages, as far as the fleeting measure and positioning of the relevant help normal for each message. The novel trust-based multicast routing convention proposed called MTAODV (Multicast Trust—based AODV) in [28] to secure against numerous attacks and improve routing effectiveness. They processed direct trust utilizing the Bayesian hypothesis and roundabout trust utilizing assessment validity and action. The fluffy rationale hypothesis was applied to fuzzify the immediate and roundabout trust esteems, and afterward, the absolute trust estimation of the hub is gotten by defuzzification. The modified AOMDV convention with an RLLMR (Reliable Low-Latency Multipath Routing) technique proposed in [29] based on multipath interface unwavering quality, equipped for deciding the reliable courses pre-emptively for VANET interchanges. The blockchain-based trust the board and data sharing answer for VANETs was designed in [30] called DrivMan. The utilization of DrivMan gives every vehicle a one-of-a-kind crypto-unique mark that was utilized to build up data provenance. Declarations gave by foundation units are abused to save the protection of the vehicles. DrivMan can be utilized as a compelling answer to forgive both data provenance and data uprightness to shrewd vehicles in VANETs for their safe and reliable activity. Another recent trust-based methodology for secure data forwarding in VANETs was proposed in [31] using artificial intelligence (AI) and trust evaluation. They used the fuzzy logic technique and neural network for the trust evaluation algorithm. Recently various VANET routing solutions [32-36] have been proposed using the trust management approach for reliable data transmission.

B. Research Motivation and Contributions

The above studies show that reliable communications can be using trust and reputation-based techniques effectively. However, considering the challenges of position-based routing related to the intersection management system, it becomes difficult to design trust-based threat detection in VANETs. The communication overhead incurred due to inefficient intersection selection mechanism along with unreliable forwarding mechanism in present solutions. It is mainly due to the high mobility of vehicles that leads to excessive data loss and increases communication costs. Therefore, the research gaps noticed in position-based and trust-based methods are summarized below:

- Inaccurate selection of intersections leads the network performance degradations regardless of optimal path availability.
- Inefficient intersection selection approach due to consideration of just immediate intersection while next intersection selection.
- The communication overhead was incurred due to an inefficient intersection selection mechanism.

- Unreliable forwarding mechanism due to the high mobility of vehicles and congestions caused by unreliable nodes leads to excessive data loss and increases communication cost.

Considering the above research gaps, we focused on intersection management free secure position-based routing in this paper in novel ARPVP protocol. The novelties of ARPVP protocol are summarized in below contributions:

- Self-trust computation model to detect the unreliable vehicles in the network before link discovery and data transmission with minimum computation burden regardless of any specialized mechanism for RSU and intersection points.
- Reliable and Stable position-based routing using the nature-inspired algorithm ACO regardless of intersection management and RSU devices monitoring.
- Extensive performance evaluation of proposed protocol with state-of-art trust-based VANET protocols by considering the different network scenarios and traffic patterns.

3 Methodology of ARPVP

The proposed protocol ARPVP has based on a trust-based approach for continuous reliability monitoring and reliable data transmission. In both cases, a trust-score is computed for each vehicle to achieve security against the various threats in VANET. As discussed earlier, the ARPVP has designed in two phases such as (1) attack detection phase and (2) position-based data transmission phase. This section presents the design of both phases.

A. Trust-based Attack Detection

Figure 1 shows the working of planned approach for attack detection. As showing in figure, after the deployment of VANET network with P number of vehicles, the process of attack detection applied on each vehicle node N. The P numbers of vehicles are deployed in $X \times Y$ size VANET network as $N = \{N^1, N^2, \ldots N^P\}$. The process of attack detection using a trust-evaluation approach has been performed the computation of the indirect trust score of each vehicle during every Time Division Multiple Access (TDMA) channel slot till to end of the simulation. Three parameters of each vehicle are computed in the trust-evaluation model like vehicle mobility, vehicle link quality, and congestion on the vehicle.

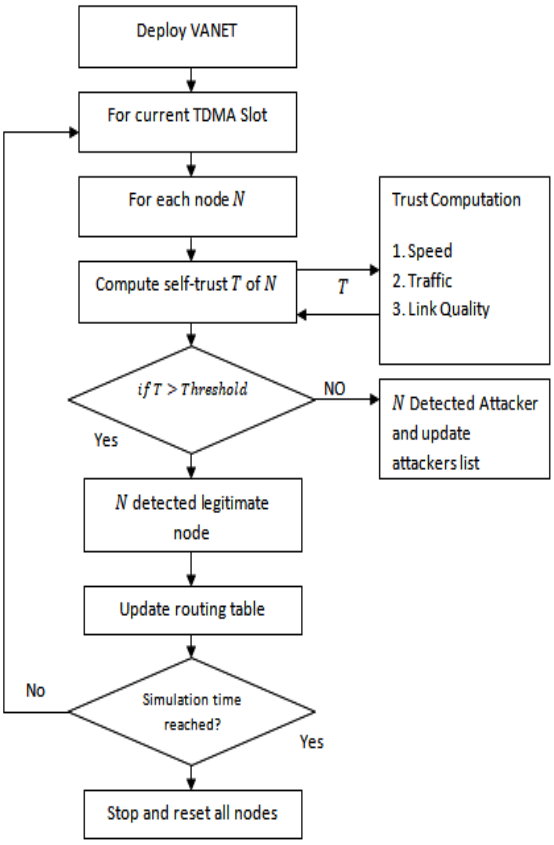

Figure 1. Design of trust-based attack detection in VANET

The speed parameter has been used to discover the stable vehicles in the network for the data relaying process. As the vehicle with high mobility is considered an unreliable node, the current speed of the vehicle is an important trust parameter for attack detection. Furthermore, due to the malicious behavior of the attacker, the Medium Access Control (MAC) layer parameter called link quality is greatly affected and leads to a poor MAC layer trust score. This trust score helps to discover the cross-layer attackers easily, therefore the aforementioned trust parameter is computed for attack detection. The final parameter is related to network load or congestion on the vehicle. Attacker nodes are frequently broadcasting the false message that creates heavy bandwidth utilization around it and leads to packets drop. Thus estimate the current bandwidth level of the vehicle helps to discover the behavior. We used all three trust parameters to compute the trust score of each vehicle and then compared it with the predefined threshold value. If the trust score of vehicle N at the current time t is less than the predefined threshold value, then it is detected as an attacker node, and then necessary prevention measures are taken. Otherwise, node N is declared as legitimate and can be available for data forwarding processing. The entire process of attack detection mathematically presented in algorithm 1.

Algorithm 1: Unreliable Vehicles Detection
Inputs $P: number\ of\ vehicle$ $threshold = 0.4$ $t: TDMA\ time\ interval$ $ST: simulation\ time$ ***Output*:** $A: attackers\ list$ $NA: Non - Attackers\ list$
1. For each TDMA time interval t 2. For each vehicle $N \in P$ 3. $T1_N^t: estimate\ the\ speed\ using\ Eq.(1)$ 4. $T2_N^t: estimate\ the\ bandwidth\ level\ using\ Eq.(2)$

```
5.    T3_N^t: estimate the link quality using Eq.(3)
6.    T_N^t: Weighted trust value using Eq.(4)
7.    If (T_N^t > threshold)
8.      'node N is legitimate and update the list'
9.          NA = {N}
10.   Else
11.     'node N is unreliable and alarm raised'
12.       A = {N}
13.   End If
14. End For
15. End For
```

As noticed in algorithm 1, every vehicle analyzed according to their trust value T computed using three self-trust parameters. These parameters computed as below:

Mobility Trust: This trust parameter returns the current moving speed of the vehicle N at time t using below equation (1).

$$T1_N^t = 1 - \frac{mobility(N)}{120} \quad (1)$$

The max speed considered for each vehicle is 120 Km/hr. This delivered the $T1_N^t$ that in range of 0 to 1. Higher the $T1_N^t$ value, better the chance to become legitimate node.

Traffic Trust: This parameter estimates the trust score of N according to its bandwidth allocation to define its behaviour in network. The computation of this parameter is concerns the two important factors such as current bandwidth requirement and allocated bandwidth. We allocated the maximum and minimum trust values to define the current level of traffic around node N.

$$T2_N^t = \begin{cases} 0.8, & if\ (BW^A + BW^D) < BW^{max} \\ 0.2, & otherwise \end{cases} \quad (2)$$

Where, BW^A and BW^D are current available and demand of bandwidth around vehicle N at current time t. The BW^{max} represents the maximum bandwidth value allocated to each vehicle in-network is 2 Mbps.

***Link Quality Trust*:** This parameter computes the MAC layer link quality trust of node N between time intervals. It is computed as:

$$T3_N^t = \frac{N_{recv}(t_{i-1}, t_i)}{N_{exp}(t_{i-1}, t_i)} \quad (3)$$

Where N_{recv} and N_{exp} total number of packets received and expected number of packets during the time interval(t_{i-1}, t_i) at node N. Higher $T3_N^t$, good chances to become legitimate node for vehicle N.

Common Trust Score: Once the three trust parameters computed for vehicle N at time t, then the common trust score estimated using the weights. This periodic trust value computed for each vehicle and compared with the predefined threshold value as shown in algorithm 1 and figure 1. It is computed as:

$$T_N^t = \left((w^1 \times T1_N^t) + (w^2 \times T2_N^t) + \left(w^3 \times T3_{Nb^i}^t\right)\right) \quad (4)$$

Where, $w^1, w^2, \& w^3$ are weight parameters applied to normalize the trust score in range 0 to 1. The selection of these values should satisfy the condition of $w^1 + w^2 + w^3 = 1$. These weight values used as $w^1 = 0.35,\ w^2 = 0.35, \& w^3 = 0.3$. T_N^t value is compared with threshold which is set to 0.4 for this protocol. This value is set through the performance analysis of proposed protocol.

B. Position-based Data Transmission

The process of attack detection is periodically updating the list of legitimate and attacker nodes in the network, which is helpful during the cycle of course disclosure and data transmission to forestall data misfortune. The course revelation fundamentally set off by any source hub S∈N that wants to send the data towards the objective hub $D \in N$. Disclosure of the steady and reliable course between the source and objective is a difficult examination issue for VANETs. The ACO used to find the ideal course by figuring the trust of each forwarder hub.

The problem of discovering the stable route is formulated by applying the ACO to search for the best relay node using trust analysis of each vehicle. The idea of the ACO remains the modeling of the ant behavior related to their ability to find the best available route from the anthill to the food source as demonstrated in figure 2 (1) where the shortest route is preferred. The process of ACO is iterative in which initially the ant broadcasted the way with pheromone, and this information utilized by other ants to select the route (figure 2(2)). The final route traveled by the ant visible when all the possible

options are evaluated (figure 2 (3)).
The main steps of ACO to select the best route are:

- Initialize the ants at the source from which the data transmission will perform.
- Construction of the acceptable alternative forwarders.
- The rule determining the probability of the ant transition from the current node to the next node.
- The rule of Pheromone update once after the selection of the best next-hop node in the network.
- Pheromone evaporation rule.

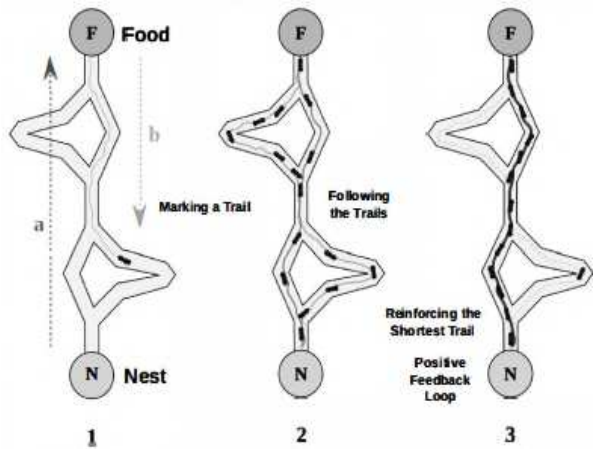

Figure 2. Illustration of ACO working

Using ACO, S triggers the reactive route formation process by finding its neighbors and broadcasting set ants At to all its neighbors. The set of ants At generated based on the number of neighbors discovered at the current node, each ant works to find the best solution among all available neighbors based on their trust score value evaluation. Similar to attack detection, the trust score is registered to utilize three key boundaries of every vehicle, for example, speed, geographical distance from the current vehicle to the next forwarder node, and traffic estimation level of a vehicle. This process has presented in algorithm 2. As showing in the algorithm, the next-hop node selected based on their current probability value computed using the parameters such as speed, geographical distance, and traffic conditions.
The best part of this algorithm is that it checks periodically for the node's behavior against the attacker's list. The node is analyzed for the selection of forwarder only if it's not belonging to the periodically updated attackers list. The trust score $T^t_{Nb^i}$ for i^{th} neighbouring node Nb^i at time t is computed as:

$$T^t_{Nb^i} = \left(\left(w^1 \times T1^t_{Nb^i}\right) + \left(w^2 \times T2^t_{Nb^i}\right) + \left(w^3 \times T4^t_{Nb^i}\right)\right) \quad (5)$$

Where, $T1^t_{Nb^i}$ and $T2^t_{Nb^i}$ computes the speed and bandwidth level trust scores as discussed in above section. The weight parameters are similar as used in attack detection algorithm. Apart from this as this position-based routing we computed the geographical distance among the two vehicles as:
The $distance^i$ based trust score for a node N^i is computed as:

$$p^1 = getPos(IV) \quad (6)$$

$$p^2 = getPos(Nb^i) \quad (7)$$

$$T4^t_{Nb^i} = 1 - \frac{|p^1 - p^2|}{\left(\frac{(X+Y/2)}{2}\right)} \quad (8)$$

Where, X and Y represents the height and width of the VANET network, the outcome value in $T4^t_{Nb^i}$ in the range of 0 to 1. Higher the $distance^i$ value of node N^i better the chance to become the next forwarder node.

Algorithm 2: Route discovery and data transmission

Inputs
S: $Source\ vehicle$
D: $Destination\ vehicle$
Nb: $Set\ of\ neighbouring\ vehicles$
IV: $investigation\ of\ vehicle$
t: $present\ simulation\ time$
ST: $simulation\ time$
Ph: $pheromone\ value$
Output:
Rt: $discovered\ route\ at\ time\ t$

1. While ST
2. At time t
3. $IV = S$
4. IV discovers the one-hop neighboring nodes Nb
5. Broadcast ants $At^i \in At$ for each $Nb^i \in Nb$
6. For each Nb^i of, upon receiving At^i
7. If $(Nb^i \neq A)$
16. $T1^t_{Nb^i}$: $estimate\ the\ speed\ using\ Eq.(1)$
17. $T2^t_{Nb^i}$: $estimate\ the\ bandwidth\ level\ using\ Eq.(2)$
18. $T4^t_{Nb^i}$: $estimate\ the\ geographical\ distance\ using\ Eq.(8)$
19. $T^t_{Nb^i}$: $Weighted\ trust\ value\ using\ Eq.(5)$
8. $T(i) \leftarrow T^t_{Nb^i}$
9. Select the next forwarder vehicle:
10. $IV = \max(index(T))$
11. End if
12. End for
13. If $(IV \neq D)$
    - 13.1. Forward At^i to IV
    - 13.2. Update pheromone value i.e. Ph
    - 13.3. Go to step 4
14. Else
    - 14.1. Construct the reveres ant and discover the route Rt
    - 14.2. Update pheromone value i.e. Ph
    - 14.3. Forward data from $S\ to\ D$
15. End if
16. End For
17. End While

Figures 3-5 illustrate the secure and dynamic data forwarding mechanism of the proposed protocol. Figure 3 shows the VANET with source vehicle and destination vehicle or base station node in the network. All other vehicles are moving across the urban area. When the source node triggers the route discovery phase, the trust evaluation of neighboring nodes performed according to algorithm 2.

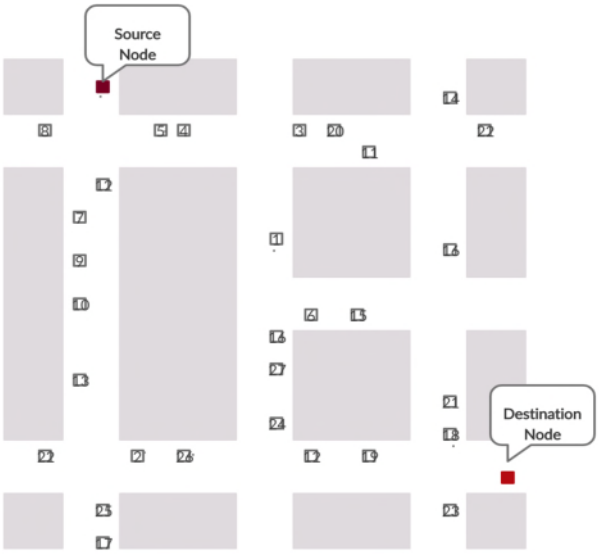

Figure 3. VANET deployment with source and destination nodes

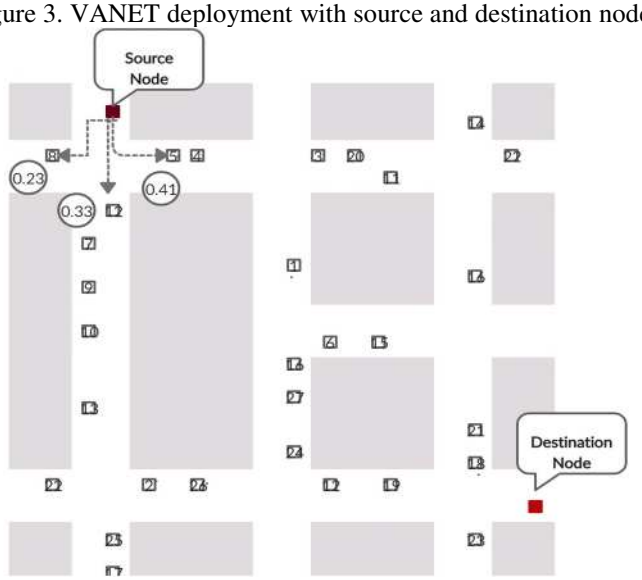

Figure 4.Trust scores evaluations to select the next forwarders

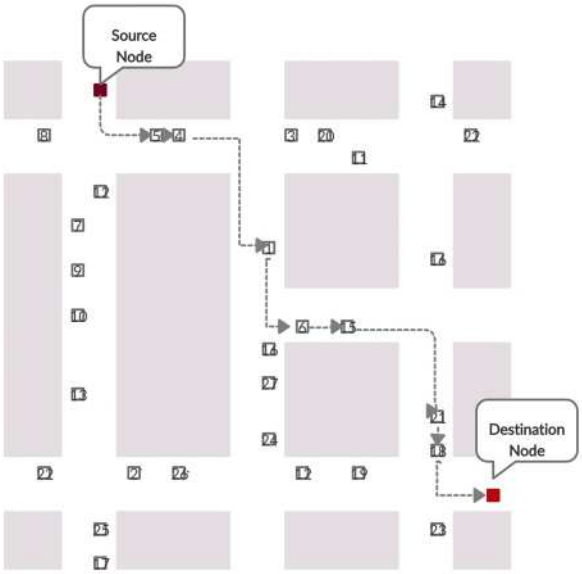

Figure 5. The path estimated between source and destination for data forwarding

As observed in figure 4, nodes 8, 12, and 5 received the requests and responded with their current trust values 0.23, 0.33, and 0.41 respectively. Node 5 is selected due to the higher trust value for vehicular data forwarding towards the intended recipient. Also, nodes 8 and 12 were part of the attacker list. Thus, the 5 becomes the next current node, and the same process is repeated to select the next forward node until the destination node has reached. Finally, figure 5 shows the final estimate path to transmit data from the source vehicle to the destination using the proposed approach.

4 Simulation Results

The ARPVP protocol is implemented and analyzed in the NS2 tool. The presentation of ARPVP protocol compared with recent trust-based routing protocols of VANET such as ART [24] and MTAODV [28] as the methodology of both protocols overlapping the concept of ARPVP and position-based routing. Also, the reason behind selecting these protocols is that they were evaluated regardless of VANET topology and RSU points. The performances of these protocols are compared using the parameters like average delay, average throughput, packet delivery ratio (PDR), and communication overhead (determines time & space complexity). The network scenarios used for the evaluations are varying numbers of vehicles (table 1) and varying mobility speed (table 2). For both scenarios, we used different mobility models namely random walk and Manhattan grid models with CBR and VBR traffic patterns. According to the simulation parameters section, A presents the results for density variations, and section B presents results for mobility variations. The simulation parameters show the presence of 10 % malicious vehicles in the network.

Table 1. Simulation parameters for density variations

Number of vehicles	50-300
CBR Traffic	6
Simulation Time	300 second
Mobility (Km/hr)	40
Attackers	10 %
Routing Protocols	**ART, MTAODV, ARPVP**
MAC	802.11p
Propagation Model	Two-Ray Ground
Area	7000 x 7000
Mobility	Random Walk
Antenna	Omni Antenna
Traffic Model	**CBR and VBR**

Table 2. Simulation parameters for mobility variations

Number of vehicles	100
CBR Traffic	6
Simulation Time	300 second

Attackers	10 %
Mobility (Km/hr)	40, 45, 50, 55, 60, 65, 70
Routing Protocols	**ART, MTAODV, ARPVP**
MAC	802.11p
Propagation Model	Two-Ray Ground
Area	7000 x 7000
Mobility	Manhattan grid mobility model
Antenna	Omni Antenna
Traffic Model	**CBR and VBR**

A. Results of Density Variations

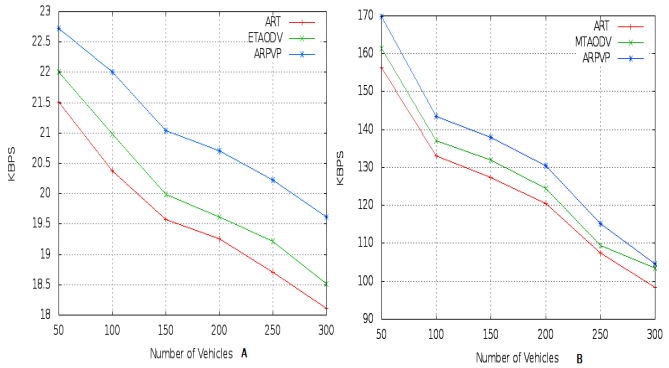

Figure 6. Average throughput evaluations for density variations (A) CBR traffic and (B) VBR traffic

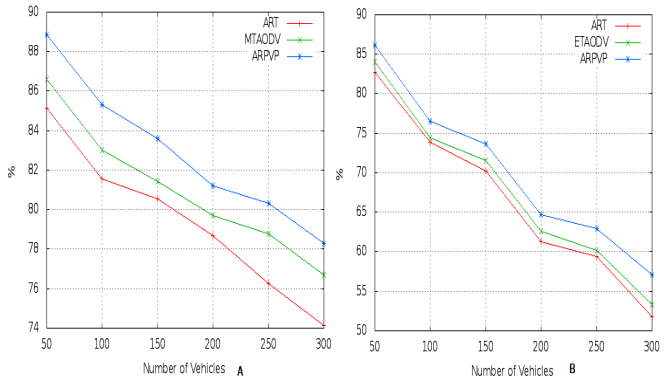

Figure 7. PDR evaluations for density variations (A) CBR traffic and (B) VBR traffic

Figures 6-9 demonstrates the results of throughput, PDR, delay, and communication overhead with varying numbers of vehicles using both CBR and VBR data traffics. From figures 6 and 7, we saw that as the network thickness builds, the exhibition of throughput and PDR diminishes because of a higher number of hops to send data from source to sink. The increased number of vehicles leads to more time to discover the forwarders and transmit data, and hence the throughput performance gets degraded. Another point that has been noticed here that the throughput ratio between CBR and VBR traffics. For VBR the traffic very much higher due to its high data rate capability of transmitting the multimedia traffic as compared to low data rate-based CBR traffic.

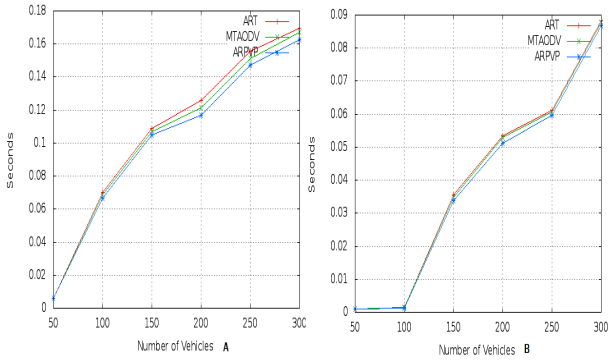

Figure 8. Delay evaluations for density variations (A) CBR traffic and (B) VBR traffic

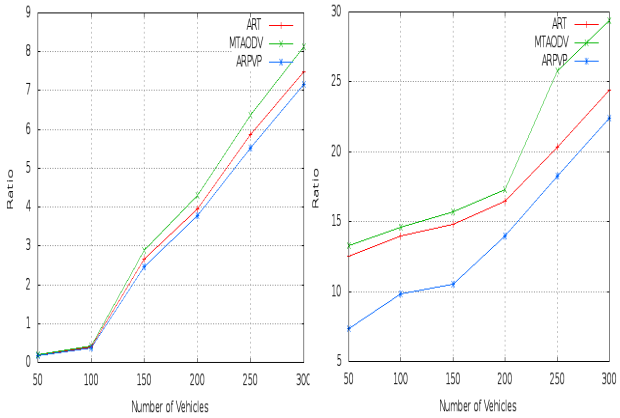

Figure 9. Communication overhead evaluations for density variations (A) CBR traffic and (B) VBR traffic

Apart from this, the throughput performance in figure 6 shows a significant improvement in proposed protocol performance as compared to ART and MTAODV protocols under the attendance of 10 % malicious nodes. It is since of the approach of discovering the reliable nodes and establishing the stable route for data transmission with periodic attack detection and alarming method. Similarly, figure 7 demonstrates the PDR performance that is overlapping the throughput performance. The existing protocols ART and MTAODV only focused on trust-based attack detection, however, it is possible that during the route discovery nodes may change their behaviors, and hence leads to unreliable communications in a network. In the proposed protocol, we applied the trust-based route establishment using ACO which resulted in the reduced number of packets dropped. Therefore, the proposed protocol achieved improved PDR and throughput using both CBR and VBR traffic patterns.

Figures 8 and 9 demonstrate the delay and communication overhead results. These results show that as the density an increasing, the delay and communication performance becomes worst. This is a possibility due to the increased number of re-transmissions caused by a higher number of vehicles in the network. The proposed protocol able to reduce the delay and communication overhead compared to both existing methods. The proposed protocol has taken a fewer number of routing packets to perform the communications because of minimum route formation operations. It leads to less communication overhead achieved compared to ART and MTAODV protocols.

B. Results of Mobility Variations

Mobility of vehicles is the vital problem of VANETs because it leads to unreliability in the network due to frequent operations of route discovery, route formation, and data transmission. The performance of VANET is significantly affected by the mobility of vehicles. Therefore, in this paper, we investigated the mobility variations and measure their effects on ART, MTAODV, and proposed protocols. Figures 10-13 demonstrate the outcomes for throughput, PDR, delay, and communication overhead respectively. From these results, the clear effect of higher mobility speed has been analyzed on all performance metrics. The increased mobility speed leads to decreased network throughput, PDR, and increased communication delay and overhead. It is mainly outstanding to the detail that severe mobility speed leads to unstable routes and hence the frequent route formation operations performed in the network.

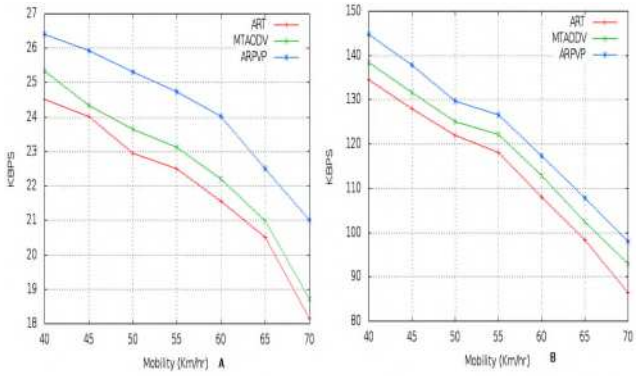

Figure 10. Throughput evaluations for mobility variations (A) CBR traffic and (B) VBR traffic

The results of throughput (figure 10) and PDR (figure 11) demonstrate that the proposed protocol achieved improved tolerance against the increasing mobility speed as we consider mobility as a key trust parameter in both attack detection and route formation process. It leads to reduced route formation tasks and re-transmissions in the network. However, the existing protocols evaluate the nodes for attack detection only, and the route formation process is non-optimal.

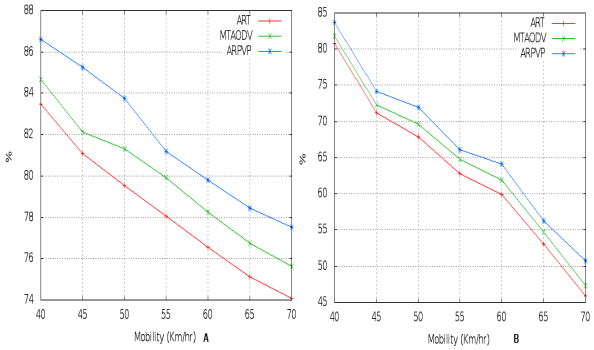

Figure 11. PDR evaluations for mobility variations (A) CBR traffic and (B) VBR traffic

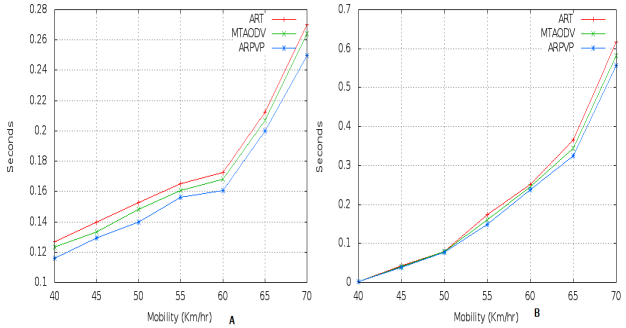

Figure 12. Delay evaluations for mobility variations (A) CBR traffic and (B) VBR traffic

The communication delay analysis by considering the mobility variations showing in figure 12 using both the CBR (A) and VBR (B) traffic patterns. The communication delay, as well as communication overhead (figure 13), is higher in the case of VBR traffic patterns as compared to CBR patterns. The proposed convention accomplished diminished correspondence delay when contrasted with existing conventions because of clear reasons uncovered in the above conversations. Along with trust-based attack detection, the reliability and robustness of the proposed protocol achieved using the optimal selection of forwarder nodes. And such functionality not available with existing protocols ART and MTAODV.

Furthermore, the communication overhead performance showing in figure 13 for both CBR (A) and VBR (B) traffic patterns disclosing that the proposed reliable and secure protocol able to keep the minimum computational overhead compared to existing protocols. As the consolidated approach used in the proposed protocol for attack detection and optimization-based method where the focus is on the discovery of more stable routes in the network which assures the guaranteed data delivery with the minimum overhead of paths formation compared to both ART and MTAODV protocols.

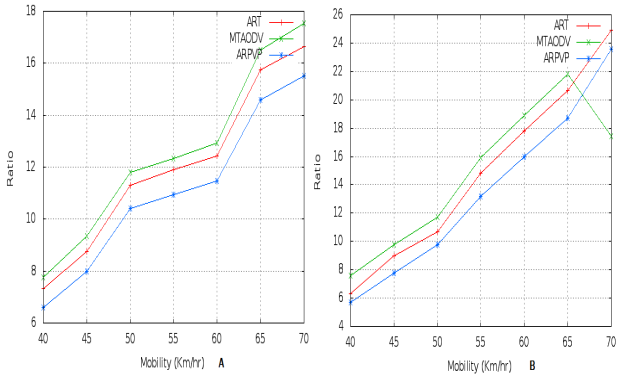

Figure 13. Overhead evaluations for mobility variations (A) CBR traffic and (B) VBR traffic

C. Time & Space Complexity

At last, the time and space complexity of all the protocols has analyzed in this section. The time complexity has analyzed using the communication delay parameter and space complexity has analyzed the average space required to perform the routing operations. The simulations were performed on Ubunto OS with RAM 4 GB and processor I3. The outcomes of time and space complexity are showing in table 3. From these results, the proposed protocol achieved a reduction in overall computation complexity compared to other protocols. It is mainly due to the reduction of operations related to route formation and frequent re-transmissions in the proposed protocol. The space requirements are computed as an average of each simulation scenario considering all TDMA time slots that show the number of routing packets generated. As the routing operations minimized in the proposed protocol, it leads to reduced space requirements as well.

Table 3. Performance of time and space complexity

	Time Complexity (Seconds)	Space Complexity (Bytes)
ART	0.1477	8994
MTADOV	0.1289	7834
ARPVP	**0.1109**	**5421**

5 Conclusion and Future Work

This paper planned the novel position-based VANET routing protocol with objectives of reliability and robustness against the various security threats. As we know that VANET is vulnerable to several challenges that affect the reliability of the network, designing a reliable routing protocol to protect against malicious behaviors of vehicles is the main motive of this paper. The protocol was proposed with a two-step approach such as trust-based attack detection and trust-based route formation. In attack detection, three parameters have been used (speed, link quality, and congestion level) to discover the malicious behaviors of vehicles. In data transmission, the route discovery has performed by trust evaluation of vehicles using three parameters (speed, congestion level, and geographical distance). The consolidated approach leads to optimal solutions for reliable VANET communications. The simulation outcomes demonstrate the ARPVP had improved the performances regarding QoS, time, and space complexities. The throughput performance of ARPVP has increased by 13 % and PDR by 12.5 %. The communication delay and overhead have reduced by 11 % and 14 % respectively using ARPVP. For future work, first, we suggest researching various types of attacks, also we recommend applying the other artificial intelligence methods for reliable route formation and data transmissions.

Compliance with Ethical Standards:

Funding: No Funding.

Conflict of Interest: All authors declares that they has no conflict of interest.

Ethical approval: This article does not contain any studies with human participants performed by any of the authors.

Data Availability Statement:

Data sharing not applicable to this article as no datasets were generated or analysed during the current study.

References

1. Chze, P. L. R., & Leong, K. S. (2014). A secure multi-hop routing for IoT communication. 2014 IEEE World Forum on Internet of Things (WF-IoT). doi:10.1109/wf-iot.2014.6803204.
2. Atzori, Luigi & Iera, Antonio & Morabito, Giacomo. (2010). The Internet of Things: A Survey. Computer Networks. 2787-2805. 10.1016/j.comnet.2010.05.010.
3. Yousuf, O., & Mir, R. N. (2019). A survey on the Internet of Things security. Information and Computer Security, 27(2), 292–323. doi:10.1108/ics-07-2018-0084.
4. Miraz, Dr & Ali, Maaruf & Excell, Peter & Picking, Rich. (2015). A review on Internet of Things (IoT), Internet of Everything (IoE) and Internet of Nano Things (IoNT). 219-224. 10.1109/ITechA.2015.7317398.
5. Sugumar, R., Rengarajan, A. & Jayakumar, C. Trust based authentication technique for cluster based vehicular ad hoc networks (VANET). *Wireless Netw* **24,** 373–382 (2018). https://doi.org/10.1007/s11276-016-1336-6.
6. Petit, J., Schaub, F., Feiri, M., & Kargl, F. (2015). Pseudonym Schemes in Vehicular Networks: A Survey. IEEE Communications Surveys & Tutorials, 17(1), 228–255. doi:10.1109/comst.2014.2345420.
7. Choi, J. Y., Jakobsson, M., & Wetzel, S. (2005). Balancing auditability and privacy in vehicular networks. Proceedings of the 1st ACM International Workshop on Quality of Service & Security in Wireless and Mobile Networks - Q2SWinet '05. doi:10.1145/1089761.1089775.
8. Hubaux, J. P., Capkun, S., & Jun Luo. (2004). The security and privacy of smart vehicles. IEEE Security & Privacy Magazine, 2(3), 49–55. doi:10.1109/msp.2004.26.
9. Kamat, P., Baliga, A., & Trappe, W. (2006). An identity-based security framework For VANETs. Proceedings of the 3rd International Workshop on Vehicular Ad Hoc Networks - VANET '06. doi:10.1145/1161064.1161083.
10. Singh, A., & Fhom, H. C. S. (2016). Restricted usage of anonymous credentials in vehicular ad hoc networks for misbehavior detection. International Journal of Information Security, 16(2), 195–211. doi:10.1007/s10207-016-0328-y.
11. Huang, D., & Verma, M. (2009). ASPE: attribute-based secure policy enforcement in vehicular ad hoc networks. Ad Hoc Networks, 7(8), 1526–1535. doi:10.1016/j.adhoc.2009.04.011.
12. Rao, Y. S., & Dutta, R. (2013). Efficient Attribute Based Access Control Mechanism for Vehicular Ad Hoc Network. Lecture Notes in Computer Science, 26–39. doi:10.1007/978-3-642-38631-2_3.
13. Kang, Q., Liu, X., Yao, Y., Wang, Z., & Li, Y. (2016). Efficient authentication and access control of message dissemination over vehicular ad hoc network. Neurocomputing, 181, 132–138. doi:10.1016/j.neucom.2015.06.098.
14. Al-kahtani Mohammed Saeed. (2012). Survey on security attacks in Vehicular Ad hoc Networks (VANETs). 2012 6th International Conference on Signal Processing and Communication Systems. doi:10.1109/icspcs.2012.6507953.
15. Lo, N.-W., & Tsai, H.-C. (2007). Illusion Attack on VANET Applications - A Message Plausibility Problem. 2007 IEEE Globecom Workshops. doi:10.1109/glocomw.2007.4437823.
16. Mahajan, H.B., Badarla, A. & Junnarkar, A.A. (2020). CL-IoT: cross-layer Internet of Things protocol for intelligent manufacturing of smart farming. J Ambient Intell Human Comput. https://doi.org/10.1007/s12652-020-02502-0.

17. Mahajan, H.B., & Badarla, A. (2018). Application of Internet of Things for Smart Precision Farming: Solutions and Challenges. International Journal of Advanced Science and Technology, Vol. Dec. 2018, PP. 37-45.
18. Salehi, M., Boukerche, A., Darehshoorzadeh, A. *et al.* Towards a novel trust-based opportunistic routing protocol for wireless networks. *Wireless Netw* **22,** 927–943 (2016). https://doi.org/10.1007/s11276-015-1010-4.
19. Mahajan, H.B., & Badarla, A. (2020). Detecting HTTP Vulnerabilities in IoT-based Precision Farming Connected with Cloud Environment using Artificial Intelligence. International Journal of Advanced Science and Technology, Vol. 29, No. 3, pp. 214 – 226.
20. Patel, N. J., & Jhaveri, R. H. (2015). Trust Based Approaches for Secure Routing in VANET: A Survey. Procedia Computer Science, 45, 592–601. doi:10.1016/j.procs.2015.03.112.
21. Yang, N.. (2013). A Similarity based Trust and Reputation Management Framework for VANETs. International Journal of Future Generation Communication and Networking. 6. 25-34..
22. Lu, Zhaojun & Wang, Qian & Qu, Gang & Zhenglin, Liu. (2018). BARS: A Blockchain-Based Anonymous Reputation System for Trust Management in VANETs. 98-103. 10.1109/TrustCom/BigDataSE.2018.00025..
23. Liu, Zhiquan & Ma, Jianfeng & Jiang, Zhongyuan & Zhu, Hui & Miao, Yinbin. (2016). LSOT: A lightweight self-organized trust model in VANETs. Mobile Information Systems. 2016. 1-15. 10.1155/2016/7628231.
24. Li, Wenjia & Song, Houbing. (2015). ART: An Attack-Resistant Trust Management Scheme for Securing Vehicular Ad Hoc Networks. IEEE Transactions on Intelligent Transportation Systems. 17. 1-10. 10.1109/TITS.2015.2494017.
25. Truong, Nguyen & Lee, Gyu Myoung. (2017). Trust Evaluation for Data Exchange in Vehicular Networks: Poster Abstract. 325-326. 10.1145/3054977.3057304.
26. Primiero, G., Raimondi, F., Chen, T., & Nagarajan, R. (2017). A Proof-Theoretic Trust and Reputation Model for VANET. 2017 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW). doi:10.1109/eurospw.2017.64.
27. Primiero, Giuseppe. (2016). A Calculus for Distrust and Mistrust. 473. 183-190. 10.1007/978-3-319-41354-9_15.
28. Xia, H., Zhang, S., Li, B., Li, L., & Cheng, X. (2018). Towards a Novel Trust-Based Multicast Routing for VANETs. Security and Communication Networks, 2018, 1–12. doi:10.1155/2018/7608198.
29. Abbas, F., Fan, P. & Khan, Z. A novel reliable low-latency multipath routing scheme for vehicular ad hoc networks. J Wireless Com Network 2018, 296 (2018). https://doi.org/10.1186/s13638-018-1292-1.
30. Javaid, U., Aman, M. N., & Sikdar, B. (2019). DrivMan: Driving Trust Management and Data Sharing in VANETs with Blockchain and Smart Contracts. 2019 IEEE 89th Vehicular Technology Conference (VTC2019-Spring). doi:10.1109/vtcspring.2019.8746499.
31. Renjith, P.N. Towards Secure Data Forwarding with ANFIS and Trust Evaluation in Wireless Sensor Networks. *Wireless Pers Commun* **114,** 765–781 (2020). https://doi.org/10.1007/s11277-020-07392-1.
32. Wang, W., Wu, L., Qu, W., Liu, Z., & Wang, H. (2020). Privacy-preserving cloud-fog–based traceable road condition monitoring in VANET. International Journal of Network Management. doi:10.1002/nem.2096.
33. Meng, Weizhi & Cofta, Piotr & Grandison, Tyrone. (2020). Editorial for special issue on security, trust, and privacy in internet of things: Challenges and solutions. International Journal of Network Management. 31. 10.1002/nem.2150.
34. Ghaffari, A. Hybrid opportunistic and position-based routing protocol in vehicular ad hoc networks. *J Ambient Intell Human Comput* **11,** 1593–1603 (2020). https://doi.org/10.1007/s12652-019-01316-z.
35. Ramamoorthy, R., Thangavelu, M. An enhanced hybrid ant colony optimization routing protocol for vehicular ad-hoc networks. J Ambient Intell Human Comput (2021). https://doi.org/10.1007/s12652-021-03176-y.
36. Balamurugan, A., Priya, M.D., Malar, A.C.J. et al. Raccoon optimization algorithm-based accurate positioning scheme for reliable emergency data dissemination under NLOS

situations in VANETs. J Ambient Intell Human Comput (2021). https://doi.org/10.1007/s12652-020-02839-6.