Received: July 9, 2019. Revised: September 12, 2019. 35

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

VTD Protocol: A Cluster based Trust Model for Secure Communication in VANET

Charles Brijilal Ruban[1]* **Balasubramanian Paramasivan[2]**

[1]*Anna University, Chennai, Tamil Nadu, India*
[2]*Department of Information Technology, National Engineering College, Kovilpatti, Tamil Nadu, India*
* Corresponding author's Email: brijilal@gmail.com

Abstract: Vehicular Ad-hoc Network (VANET) has wide application in developed/developing nations, for the effective management of vehicular traffic, and inter vehicular communication. In vehicular communication, the data includes traffic alert and safety warning. In most of the previous research achieved better quality in VANET routing. In some research, the researchers also proposed the security model for the secure transmission of these data. Instead of giving importance to the security of these data, trust ability of data and data transmitter is essential in VANET communication. In this paper a new protocol called Virtual Trust-ability Data transmission (VTD) is proposed for the effective handling of VANET. In the proposed protocol, three stages are used in the first stage a virtual topology is crated using a simple clustering technique. Then in the second stage the trust ability of every node or vehicle is analysed. In the last stage, the data are transmitted via the trusted vehicle and remove the false data from the communication. Then the performance of the proposed VTD protocol is analysed based on packet failure rate, bandwidth utilization and network scalability. The proposed VTD provided 94% of packet delivery ratio with 6% of the average packet failure. Similarly, the other performance also improved as compared to the conventional technique. So, it is clearly proving that the proposed VTD protocol can become a better alternate for the trust aware routing in VANET.

Keywords: Vehicular ad-hoc network, Trust ability analysis, False data detection, VANET routing, Trust model.

1. Introduction

In Vehicular communication the VANET plays a major role, for providing the effective communication between vehicles [1]. VANET is one of the subcategories of the mobile ad hoc networks (MANET), so its major operation is similar to MANET [2]. But in case of VANET, the nodes or Vehicle move on a specific path, instead of random path as in MANET [3]. The VANET is penetrated to provide communication between vehicles, these communication data include safety alert or traffic information [4]. In road safety and traffic management, the vehicles are programmed to sense and transfer the data related to the traffic and safety to the other vehicles [5, 6].

An effective VANET can enable high safety and traffic management, for the vehicle transportation [7]. But in this VANET some malicious nodes may interrupt the smooth communication, by creating issues like false data propagation, message suppression and denial of service [8, 9]. In order to provide the secure data delivery, the researchers have proposed many systems including secure crash reporting, safety message sharing and cooperative collision avoidance etc. [10, 11].

The researchers widely concentrated on quality based VANET and there is a less study or technique for the effective mechanism for the detection of false data. The false data can be created either by the malicious node or attacker, it can misguide the vehicle and may lead serious issue due to the VANET. Hence it is very essential to develop a suitable technique for the detection of false data by enabling trusted communication in VANET.

Thus, the proposed work is concentrated to develop a novel trust model for the effective communication in VANET by enabling trust ability.

In this work we proposed a novel system for trust-based communication in VANET called Virtual Trust-ability Data transmission (VTD) protocol. The contribution of the proposed work is as follows;

1. The virtual topology for the VANET will be created using the k-means algorithm.
2. Then the trust-ability of every node is analysed using the proposed trust model clearly described in section 3.2.
3. Finally, the data is transmitted through the trusted node and eliminate the false data from the communication.

The proposed protocol is implemented using MATLAB and its results are analysed based on the packet failure rate, bandwidth utilization, and network scalability etc. The rest of the chapter is organized as the proposed VTD protocol is described in section 2. The implementation results and discussion of the proposed protocol is given in section 3. The section 4 gives the conclusion.

2. Related work

In the section some the recent research related to the trust based VANET routing is listed. In order to provide safe and reliable communication in VANET, K. Rostamzadeh et al. [15] have propose a trust-based framework. In [16], N. Kumar, and N. Chilamkurti have proposed a trust aware Collaborative Learning Automata based Intrusion Detection System for VANET. M.H. Eiza et al. [17] have proposed a novel routing system for VANET, by concentrating the security, reliability and QoS. R. Hussain et al. [18] proposed a secure and privacy-aware service for the VANET based cloud service. Ahmed, S., et al. [19] have presented a VANSec technique for the security-aware routing in VANET. P. Yang et al. [20] have proposed a socially aware security message forwarding mechanism for the VANET communication.

Xia, H., et al. [21] have proposed a novel trust-based multicast routing protocol (TMR) to defend against multiple attacks and improve the routing efficiency. In this trust model, direct trust was calculated based on Bayesian theory and indirect trust is computed according to evaluation credibility and activity. Hasrouny, H., et al. [22] have proposed a security framework based on vehicles behaviour analysis. In this framework a Hybrid Trust Model (HTM) was defined and a misbehaviour detection system (MDS) where a trust metric is assigned to every vehicle depending on its behaviour. Goudarzi, F., et al. [23] have presented a traffic-aware position-based routing protocol for vehicular ad hoc networks (VANETs) suitable for city environments. Krundyshev, V., et al. [24] have discussed information security problems in transport networks VANET, a subtype of Mobile Ad hoc NETwork (MANET) in which moving vehicles were considered as networks hosts with wireless communications. Sugumar, R., et al. [25] have proposed a trust-based authentication scheme for cluster-based VANETs. The method proposed in [25], the vehicles were clustered, and the trust degree of each node is estimated. The trust degree was a combination of direct trust degree and indirect trust degree. Based on the estimated trust degree, cluster heads are selected. Then, each vehicle was monitored by a set of verifiers, and the messages are digitally signed by the sender and encrypted using a public/ private key as distributed by a trusted authority and decrypted by the destination. This verified the identity of sender as well as receiver thus providing authentication to the scheme.

But in the literature, in the existing systems [16, 19, 22] intrusion and malicious attacks were found using the trust model. In some techniques [17, 21] the natural inspired soft computing techniques are adopted to achieve the trust ability in the VANET routing. The techniques in [17,21] are not simple and not easy to implement in live implementation, because the VANET has the fast-moving nodes, hence the computation steps should be reduced to achieve better performance.

3. VTD protocol

The VTD protocol is proposed for the effective, handling of VANET communication. It is used enable the trust-ability in data communication and to remove the false data. The architecture of the VTD protocol is given in Fig. 1 and the protocol includes three phases, such as;

1. Virtual Topology
2. Trust-ability Analysis
3. Data Transmission

The major intension of this system is to receive and transfer a data based on its trust-ability. In this framework messages will be examined in a distributed and collaborative model. The broadcast distance of a message is depending on its strength. For example, the messages broadcast by normal mode have a good strength so it can travel long distance, while the same time messages broadcast by the malicious node is low strength, so it can travel minimum distance. A trust model or trust-ability model is proposed to evaluate the quality of the message.

Thus, the trustworthiness value is related to the

Received: July 9, 2019. Revised: September 12, 2019.

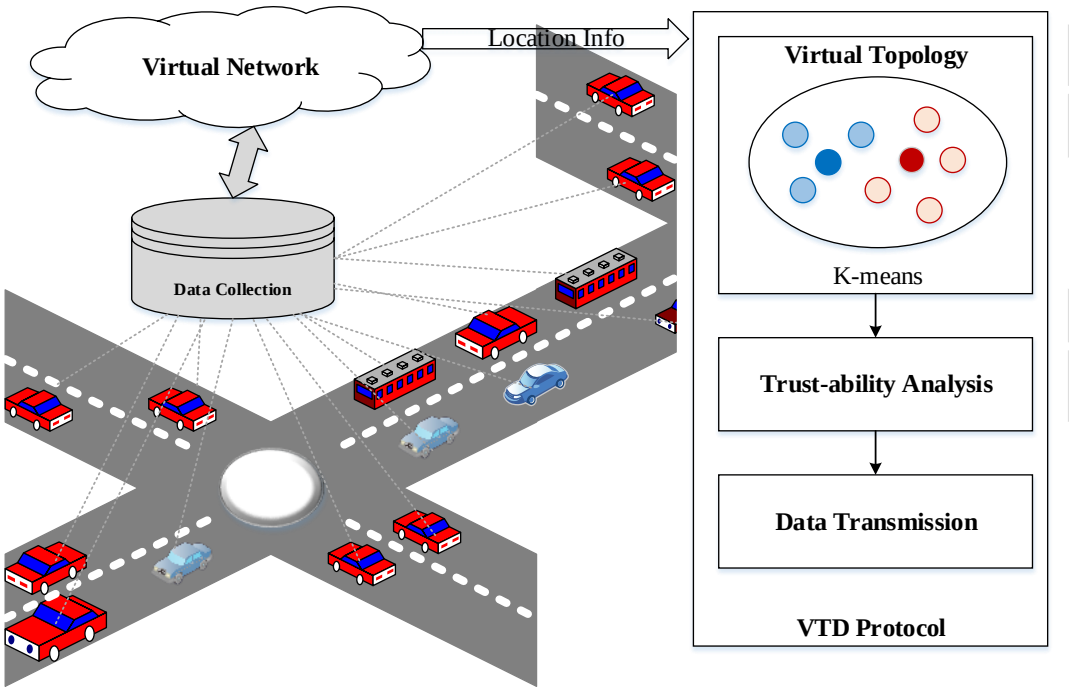

Figure.1 Architecture of the VTD protocol

message quality and is used for the message quality analysis. In this approach every node has an analysis module; the main role of analysis module is generating a trust opinion, whenever it receives the packet and sends the feedback to the sender. During the time of messages broadcast every message gets a set of trust suggestions. Moreover, every node has an action module; the main role of action module is whenever node receives the message it will decide to trust or mistrust the message based on the list of trust suggestions. Along with the trust modelling on message, the behaviour of the vehicle nodes also computed based on node to node approach.

In this trust-based framework three types of messages are used, they are sender message (SM), trust suggestion message (TM) and aggregate message (AM). The sender node will create a sender message (SM). The sender message (SM) consists of {affair, trust, time and location}. In which the trust value is within the range of 0 to 1 for reporting affair. If the trust value is high, then it is indicated that the sender is trusted among the reported affair. The time and location information can be collected using GPS, it helps to determine the geographical coordinates of vehicle at the time '*T*'. The message trust suggestion is denoted as S it includes the reaction and trust value, in which the reaction gives the suggestion, i.e., S= [*reaction, trust*], where, *reaction* $\in$ {*suggestions, suggestions1*} and *trust* $\in$ [*0, 1*]. The message trust suggestion is used to evaluate the quality of sender and its message. Then in the assessment phase, the reported affair is compared with the present data. The present data is collected by using the sensors connected in the vehicle or own local database. The aggregated message contains both the sender message and the trust suggestion by all the nodes are in the form of list. The format of aggregated message is as *AM*= [*SM, O1, O2… On*].

3.1 Virtual topology

The VANET is a type of MANET, these are self-organizing network. So, these networks do not have any specific topology while network creation [12]. Unlike MANET, the nodes in the VANET are moves on a specific path. So, it is difficult to create and maintain a fixed topology for long time. Hence to enable the self-organizing and configuring of topology the virtual topology is employed. In virtual topology a simple and effective clustering technique called k-means algorithm is used. The k-means algorithm performs distance-based clustering based on Euclidean distance function. The steps included in the virtual topology creation using k-means algorithm is as follows [13];

Initialization: In this step initialize the current location of the nodes or vehicles exists in the network. The location information usually contains the latitude and longitude value of the node at the particular instance. In vehicular network, the location of nodes

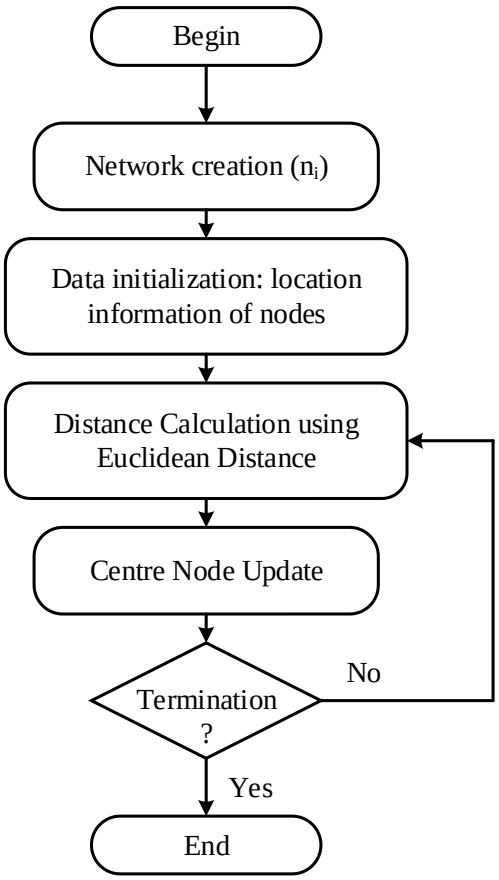

Figure.2 Flow chart for virtual topology creation

is rapidly changing due to the fast mobility. Hence the locations for a specific duration is observed and based on the speed the future location is noted for the further analysis.

Centroid Update: The average position value of all the nodes in the group is considered as the centroid and is updated as the new centroid. In the first iteration, a random centroid point chosen for the processing the grouping. The k value of k-means algorithm denotes the number of clusters, the number of clusters is equal to the number of centroids.

Grouping based on Euclidean distance: The distance between the centre node and the other nodes are calculated and closer distance nodes are gathered under the same centre node. Hence the nearer nodes are gathered into same cluster.

Termination: The above three steps are repeated till, to obtain the same centroids or centre node in subsequent iteration. The iteration is also terminated while obtaining the number of nodes in the both the clusters. The flow chart for the virtual topology creation is given in Fig. 2.

3.2 Trust-ability analysis

This section clearly states that, how the nodes effectively calculate the trust suggestions by the nodes about the message is aggregated and is broadcasted in VANET. Moreover, this section clearly demonstrated how the trust suggestions help a particular node to take decision that, whether accept or reject the sender message.

Relay Control Model: A node is decided to act as relay based on the suggestions of majority nodes in the network. The message will be accepted only if most of the nodes trusted that message else it will be rejected. Normally N denotes set of nodes in the network whose trust suggestions are mentioned as "*trust*", $N = (j|\ ID_j \in AM$ and $S_j = [trust, c_j] \in AM)$ and N be a set of nodes whose trust suggestions are "*trust*^{1}", $N = (j|\ ID_j \in AM$ and $S_j = [trust^1, c_j] \in AM)$. Every cluster has a cluster head, the cluster head is responsible to calculates the worth (*W*) of 'trust' and 'trust^1' suggestions as follows,

$$W_{trust} = \sum j \epsilon N\ c_j T_j\ ;\ W^1_{trust} = \sum j \epsilon N\ c_j T_j \quad (1)$$

The value trust $T_j \geq \tau$, where τ is a threshold value assigned by the CH, $C_i \in [0,1]$ is the confidence provided by node *j* and T_j is the node-to-node trust of node j. The node-to-node trust is explained in the following sections. Messages will be accepted only if the following condition is satisfied.

$$\frac{Wtrust}{Wtrust + Wtrust^1} \geq 1 - \varepsilon \quad (2)$$

where $\varepsilon \in [0,1]$ is a threshold value set by the cluster head to indicate the highest error rate allowed. In which, 'ε' is used in the protocol to make a decision based on data type, situation and current environment, example network failure, heavy traffic, accident, etc.

Action Module: The action module is responsible to direct for a node to take decision on sender message based on the suggested trust information. After calculating the aggregated trustworthiness value of sender message, it is directed towards the action set [follow, follow^1]. The action module of a node N calculates,

$$T_{AM} = \frac{C_S + \sum_{j \in N} C_j - \sum_{j \in N^1} C_j}{1 + |N| + |N^1|} \quad (3)$$

Where *AM* denote aggregated message, *N* denotes the trust node based on the trust suggestion, N^1 denote the node who grant trust suggestions of 'distrust', and *S* denote the actual sender. Also T_{AM} denotes the aggregated trustworthiness of the message T_{AM}. Sender's confidence about the sender message is denoted as $c_s \in [0,1]$, $c_j \in [0,1]$ represents the confidence value by node *j* in the trust suggestion,

and $T_{AM} \in [-1,1]$. The sender has various roles from the nodes which are supplies trust suggestions, sender worth factor $\gamma > 0$. It decides the level of worthiness of the sender. Since the node's reliability may changes, this system implemented a node-to-node trust model. Each node j is appended with a trust metric $T_j \in [0,1]$. To calculate the aggregated trustworthiness of the message AM, sender worth is added with the trust worthiness of each node as given below.

$$T_{AM} = \frac{\gamma C_s T_s + \sum_{i \epsilon N} C_i T_j - \sum_{i \epsilon N'} C_i T_j}{\gamma T_s + \sum_{i \epsilon N} T_j + \sum_{i \epsilon N'} T_j} \quad (4)$$

Where $\tau \in (0, 1)$ is the threshold value of trust set by every node N. The trust threshold value assists to reject the nodes which are having low trust value. In general, the value of 'τ' is chosen closer to 1, for considering the highly trusted node from the trust suggestion. In live communication the 'τ' is calculated based on the trust suggestions availability. The τ value is directly proportional to the number of trust suggestions. The action module is responsible to apply a mapping action i.e.., Action: T_{AM} = (*follow, not follow*) it converts the trustworthiness of the message into an action. If $T_{AM} >= \ddot{A}$, then *Action = follow*, else *Action=not follow*, where the action threshold value is set as $\ddot{A} \in (-1, 1)$. The value $\ddot{A}$ will be personalized by each node. The value of high action threshold express that the node is more vigilant of pursuing other nodes.

Node-to-Node Trust Module: The trust-ability of every node in the VANET is calculated based on the trust metric. The cumulated trust metric is calculated based on the experience as well as role-based trust metric. The node to node trust level of node *j* is denoted by $T_j \in (0, 1)$.

If ($T_j = T_j{}^r$) {
    Node j has a task
} *else* {
    $T_j = f(T^e_{j,n})$
}

where $T_j{}^r \in (0, 1)$, is represents the role-based trust value of node j, also $T^e_{j,n} \in (-1, 1)$, is the node *j*'s experience-based trust from the node n's appearance. By applying a mapping function map the value of T^e to the same level of T^r. We know that, most of the vehicles are used for personal usage; only a few numbers of vehicles have their particular commitment in the traffic system for example police cars. Different categories of trusts are assigned to do different tasks.

The authorities are responsible to assign the tasks. The various authorities, such as law enforcement, traffic patrols, and central or state police vehicles are assigned to have high trust level. In this approach T^r, is assigned as a more level of trust. The agent nodes are continuously monitoring the road conditions via radio, television, newspaper, mobile phone, traffic police, etc., are the second most level of trust. $T^r = 0.99$ is assigned as second more level of trust. The agent nodes should be well known about the road conditions and the traffic levels of their respective area. For example, local people, auto drivers and taxi drivers have many years of driving experience in that particular area, so they are well known about the traffic and road conditions. The third most level of trust. The $T^r = 0.98$ is assigned to the agent nodes. $T^r = .95$ is assigned to the nodes, which are having no task in the network.

To reflect a node's trust weight dynamically, the experience-based trust metric method is used. All the nodes maintain the trust weight value of other nodes by evaluating the behavior of other nodes. The node *j*'s experience-based trust from *n*'s perspective is denoted as $T^e_{j,n}$, the value should be in the limit of $(-1,1)$. The notation $T^e_{j,n}$ is simplifying as T as following. The value is adjusted if node *j*'s trust opinion is directing to a correct value n, the node n increases the trust of *j*.

$$T \leftarrow \begin{cases} \lambda^{-t}(1 - c\beta)T - c\beta & if \ T < 0 \\ \lambda^{t}(1 + c\beta)T - c\beta & if \ T \geq 0 \end{cases} \quad (5)$$

Else the T value is decreases by

$$T \leftarrow \begin{cases} \lambda^{t}(1 + c\alpha)T + c\alpha & if \ T \geq 0 \\ \lambda^{-t}(1 - c\alpha)T + c\alpha & if \ T < 0 \end{cases} \quad (6)$$

In the above equation $\alpha, \beta \in (0, 1)$ and both are decrement and increment factors. The $h \in [0, 1]$ is represents the hope value placed by node *j* in the message, $\lambda \in (0, 1)$ is represents the forgetting factor, and $t \in [0, 1]$ is represents the time difference between the previous and present interaction. The experience-based trust is scalable, so the number of nodes increases will not affect the efficiency. It frequently updates the nodes trust weight value. The trust calculation is linear with respect to the number of times received a trust suggestion from a node. The most recent trust suggestions values are store and used for further calculation. The hope 'h' is added since all the nodes including sender node have a different task in the message's trust weight by keeping different hope values

3.3 Data transmission

In this phase the data transmission begins in the VANET, the packet format of the data transmission is given in Fig. 3. The packet format of VTD has four filed, the first field has the sender or source id, the second field is for receiver or destination id, third field gives the trust value of the sender node, and the fourth field has the actual message. Whenever a node sends a data to the node, the receiver verifies the trust value and compare it with the threshold value. If the value is greater than the threshold the data will accepted else discard the data.

Cluster-based routing mechanism helps to get good trust suggestion aggregation. Since the environment is highly dynamic assuring the stability is the major problem in VANET. The Cluster-based routing mechanism helps to achieve good stability in vehicular ad-hoc networks.

In literature, many techniques have proposed for the cluster-based routing to enable scalability in vehicle to vehicle communication. In cluster-based communication, the nodes are gathered into multiple groups or clusters, and the cluster node acts as relay to main scalability. The message aggregation is formed based on the efficient and secure aggregation scheme.

Initially the nodes (vehicles) are gathered into various clusters. As shown in the above figure, the nodes are groups into ten clusters, namely C1 to C10. In each cluster C_j, the cluster nodes are responsible to select their cluster head. Cluster Head (CH) should be selected based upon the trusty nodes. The node which is at minimum distance and which maintains maximum trust degree will be selected will be selected as a cluster head. A sender node in a cluster-1 have a message 'SM', to propagates to its neighbor nodes whose will give trust suggestions.

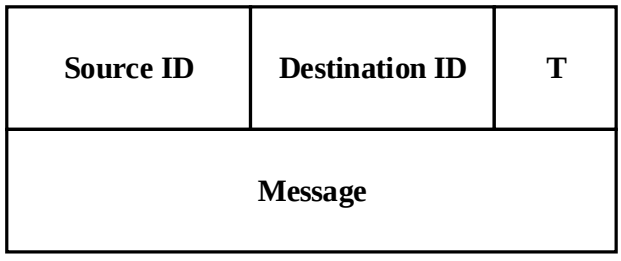

Figure.3 Packet format

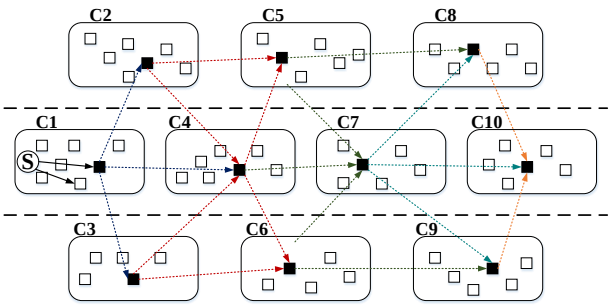

Figure.4 Cluster based message propagation

Now the cluster head collects the trust suggestions Sj from all the neighboring nodes of sender. After that CH will aggregate all the suggestions and formed an aggregated message (SM). CH-1 broadcast AM to its neighbor clusters C2, C3 and C4. The CH-2, CH-3 and CH-4 received the aggregate message and propagate to its cluster member. All the members of C2, C3 and C4 will give their trust suggestions to its corresponding CHs. Now the CH will aggregate all the trust suggestions and form a new aggregated message. Also, the CH will compute a relay decision that relay AM to the next hop cluster C5, C6 and C7.

VTD Protocol is a trust-based based routing system for VANET, it executes in three steps. The detail procedure of VTD protocol is described above and its performance is compared in the next section.

4. Results and discussion

In the proposed study, the major intension is to develop a suitable technique for the controlling of VANET data transmission to enable trust-ability. Hence the VTD protocol is proposed for providing trust-based communication in VANET.

The proposed VTD protocol is implemented using MATLAB in windows platform. The proposed system is analysed based on the performances such as packet failure, bandwidth utilization and network scalability. The simulation parameter of VANET using VTD protocol is given in Table 1.

The simulation is conducted in 100x100 m^2 with 100 vehicles, a random map is created using MATLAB. The node communication is executed over radio frequency of 2.47GHz with 50m range and the channel bandwidth is 2Mbps. The network created using MATLAB is given in Fig. 5.

The Fig. 5 shows the network created using MATLAB, in which the dot (•) denotes the data vehicle or node. In this network, we have included 100 vehicles moving on the path.

Table 1. Simulation Parameter

Parameter	Range
Number of Vehicle/Node	100
Area	100x100m2
Propagation model	Two Ray Ground
Vehicle speed	0-50 km/hr
RF	2.47GHz
Range	50m
Bandwidth	2Mbps
Number of clusters	4

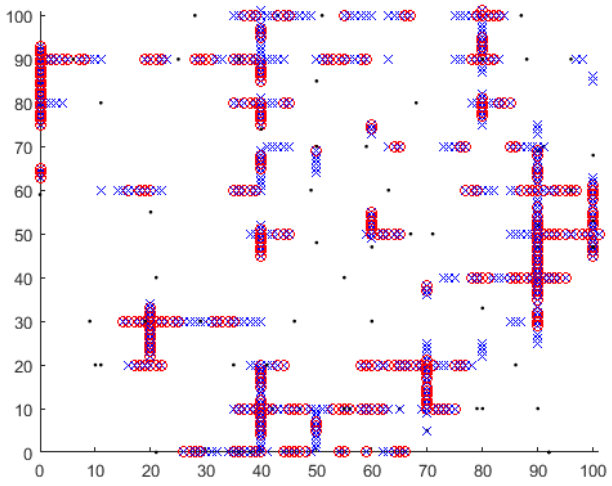

Figure.5 Network creation

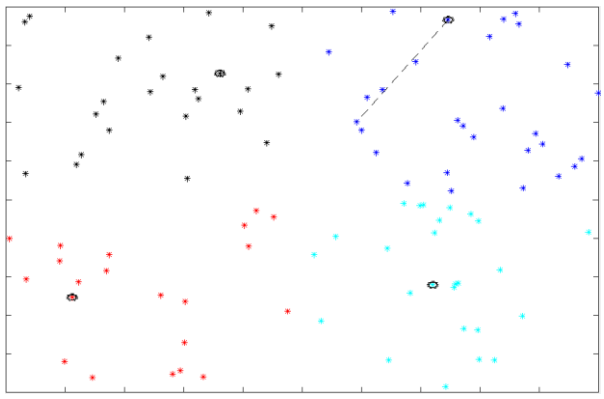

Figure.6 Virtual topology and trust-ability analysis

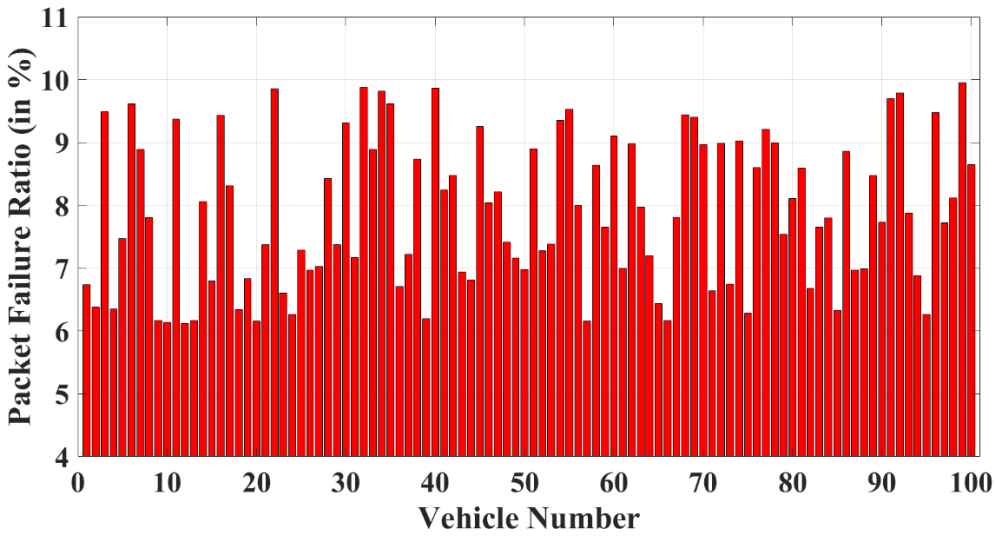

Figure.7 Packet failure ratio

Then the virtual topology is crated with four clusters and is given in Fig. 6. Fig. 6 shows the virtual topology created based on the data obtained from the previous stage. The topology is created with four clusters and each cluster has a centre node to analysis the trust ability.

The nodes are represented as "*" and the centre nodes are represented as marking extra circle over the node. The four clusters are differentiated by spotting different colours. Then the process of trust ability analysis is given in Fig. 6.

In the trust-ability analysis, the centre node is sent and receive the sample packet to analysis the trust level of the node using Eq. (1). In the Fig. 6, the dotted line between centre node and cluster nodes indicates that the communication for trust analysis. The packet failure ratio is given in Fig. 7.

The packet failure ratio or the packet loss ratio is the measure of number of packets lost to the total number of packets transmitted. Here the failure ratio measured by every node is given in the Fig. 8. It is clear that more than 90% of packets are deliver so the loss is reduced less than 10%. The packet loss ratio by proposed and existing Named Data Networking (NDN) technique [26] and SASMF [21] is analysed and is given in Fig. 9.

The Fig. 8, clearly shows that the proposed VTD protocol has reduced the average packet failure ratio form the normal VANET communication. Hence it is evident that, due to the penetration of false data elimination, there is no impact on the packet delivery and the proposed technique enhances the packet delivery ratio. The bandwidth utilization is given in Fig. 9.

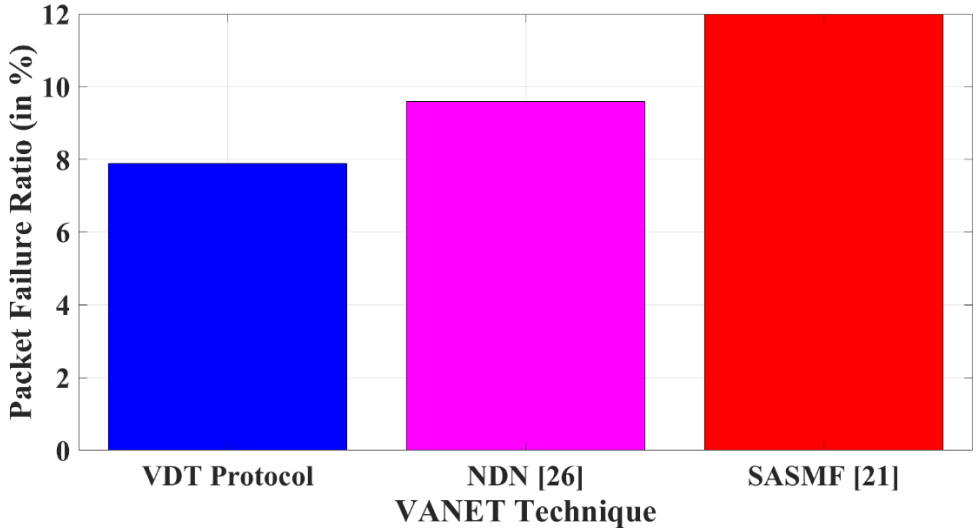

Figure.8 Comparison of packet failure ratio

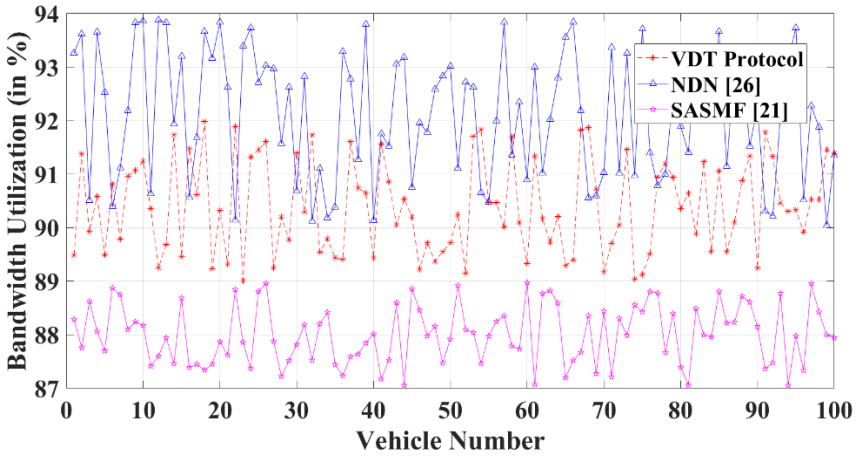

Figure.9 Bandwidth utilization with and without VTD protocol

The Fig. 9, clearly shows that the bandwidth with VTD protocol is utilized effectively comparing the normal VANET. The normal VANET utilized about 94% of bandwidth, while the VTD protocol reduces it and utilized up to 92%. Hence the penetration of VTD protocol in VANET effectively managed the bandwidth utilization. In Figs. 10 and 11 the network scalability is compared. The network scalability is evaluated based on the response time and throughput. While increasing the number of users in the network the average response time and throughput are calculated and is plotted in Figs. 10 and 11 respectively.

The Figs. 10 and 11 give the comparison of response time and throughput respectively. These comparison helps to show the scalability of network by varying the number of nodes or vehicle. The comparison shows that the performances are getting degrades while increasing the number of nodes, among the other technique with the aid of VTD protocol the performance is better and achieved better scalability. Thus, the performance analysis, suggest that the VTD protocol for the trust-based communication in VANET performed well and achieved better performance in terms of both packet failure rate, bandwidth utilization and scalability. So, the proposed techniques are better than the NDT and other techniques. Hence for the effective VANET communication the VTD protocol can enable additional benefit as the false data elimination.

5. Conclusion

The usage of VANET is increasing, for providing real time traffic alert and emergency warning to the vehicles moving on a specific road map. The penetration of malicious node or attacker may create the fake information to misguide the vehicles or vehicular nodes. This can be avoided by developing an effective false data detection technique. Thus, the

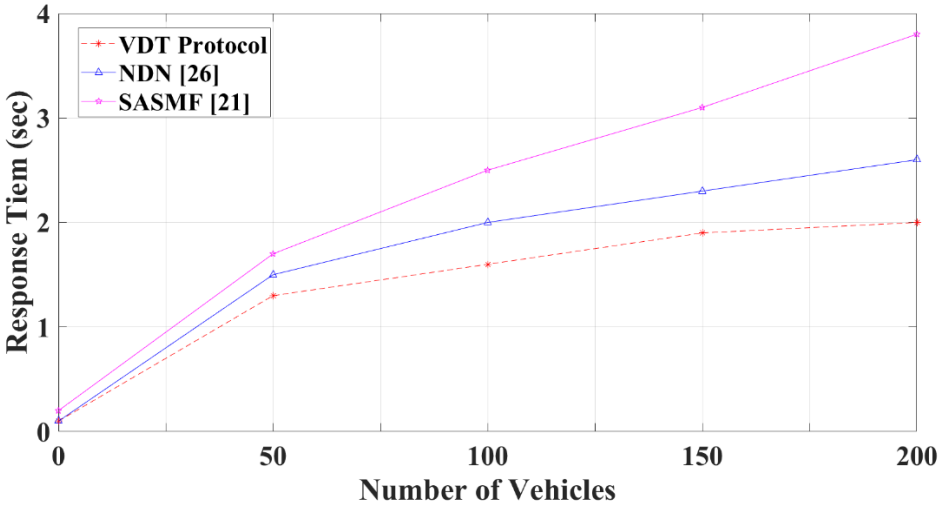

Figure.10 Response time comparison

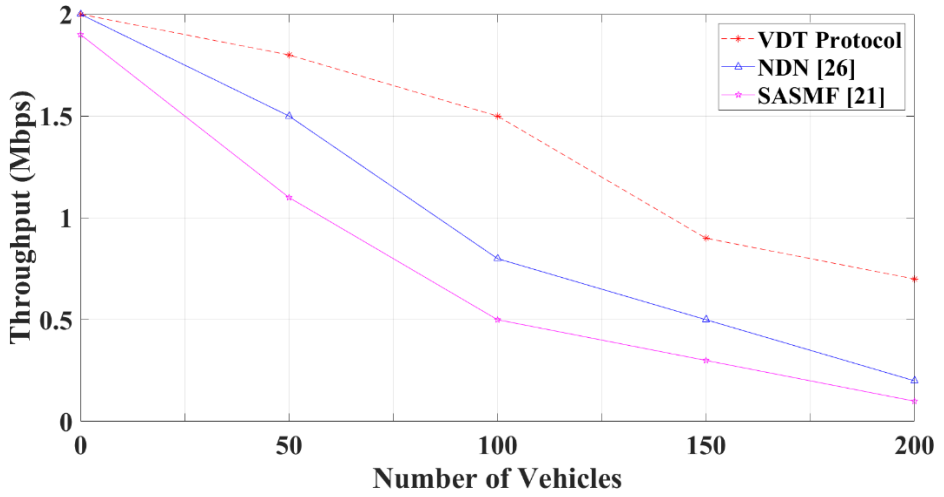

Figure.11 Throughput comparison

proposed VTD protocol enables the trust-ability based data transmission and eliminates the false data. The proposed techniques include three major phases. In the first phase the virtual topology is created using the k-means clustering. In the second phase the trust-ability of every node is analysed. In the third phase the trust data is transmitted, and the false data are eliminated. Then the proposed system is implemented using MATLAB and the performance with and without the VTD protocol is analysed. The performances such as packet failure ratio, bandwidth utilization and network scalability analysis prove the effectiveness of the proposed technique. The packet failure ratio of the proposed VTD protocol is 6%, which is nearly 4% less than the other techniques. The response time of VTD protocol is 1.25sec and 2sec while the usage of 50 and 200 nodes respectively. This is almost 2sec less than the SASMF technique. Similarly the throughput of the proposed technique is better than the other two techniques. Thus the proposed VTD proves its effectiveness for the false data detection in vehicular network. Ultimately, the proposed VTD protocol is suggested for the VANET communication with trust-ability and false data elimination.

Reference

[1] G. S. Khekare and A. V. Sakhare, "A smart city framework for intelligent traffic system using VANET", In: *Proc. of 2013 International Mutli-Conference on Automation, Computing, Communication, Control and Compressed Sensing*, pp. 302-305, 2013.

[2] Y. Toor, P. Muhlethaler, A. Laouiti, and A.D. L. Fortelle, "Vehicle ad hoc networks: Applications and related technical issues", *IEEE Communications Surveys & Tutorials*, Vol. 10, No. 3, pp. 74-88, 2008.

[3] F. Li and Y. Wang, "Routing in vehicular ad hoc networks: A survey", *IEEE Vehicular*

technology magazine, Vol. 2, No. 2, pp. 12-22, 2007.

[4] K. C. Dey, A. Rayamajhi, M. Chowdhury, P. Bhavsar, and J. Martin, "Vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication in a heterogeneous wireless network–Performance evaluation", *Transportation Research Part C: Emerging Technologies*, Vol. 68, No. 1, pp. 168-184, 2016.

[5] F. Dressler, H. Hartenstein, O. Altintas, and O. K. Tonguz, "Inter-vehicle communication: Quo vadis", *IEEE Communications Magazine*, Vol. 52, No. 6, pp. 170-177, 2014.

[6] D. J. Fagnant and K. Kockelman, "Preparing a nation for autonomous vehicles: opportunities, barriers and policy recommendations", *Transportation Research Part A: Policy and Practice*, Vol. 77, No. 1, pp. 167-181, 2015.

[7] J. A. G. Ibanez, S. Zeadally, and J. C. Castillo, "Integration challenges of intelligent transportation systems with connected vehicle, cloud computing, and internet of things technologies", *IEEE Wireless Communications*, Vol. 22, No. 6, pp. 122-128, 2015.

[8] C. Englund, L. Chen, A. Vinel, and S. Y. Lin, "Future applications of VANETs", *Vehicular ad hoc Networks*, pp. 525-544, 2015.

[9] J. C. Castillo, S. Zeadally, and J. A. Guerrero-Ibañez, "Internet of vehicles: Architecture, protocols, and security", *IEEE Internet of Things Journal*, Vol. 5, No. 5, pp. 3701-3709, 2017.

[10] F. Cunha, L. Villas, A. Boukerche, G. Maia, A. Viana, R. A. Mini, and A. A. Loureiro, "Data Communication in VANETs: Protocols, applications and challenges", *Ad Hoc Networks*, Vol. 44, No. 1, pp. 90-103, 2016.

[11] S. Bitam, A. Mellouk, and S. Zeadally, "VANET-cloud: a generic cloud computing model for vehicular Ad Hoc networks", *IEEE Wireless Communications*, Vol. 22, No. 1, pp. 96-102, 2015.

[12] S. Karthick, S. Perumal Sankar, and Y.P Arul Teen, "Trust-Distrust Protocol for Secure Routing in Self-Organizing Networks", In: *Proc. of 2018 International Conference on Emerging Trends and Innovations in Engineering and Technological Research (ICETIETR)*, pp. 1-8, 2018.

[13] S. Karthick, "TDP: A Novel Secure and Energy Aware Routing Protocol for Wireless Sensor Networks", *International Journal of Intelligent Engineering and Systems*, Vol. 11, No. 2, pp. 76-84, 2018.

[14] S. Karthick, E. Sree Devi, and R.V. Nagarajan, "Trust-distrust protocol for the secure routing in wireless sensor networks", In: *Proc. of 2017 International Conference on Algorithms, Methodology, Models and Applications in Emerging Technologies (ICAMMAET)*, pp. 1-5, 2017.

[15] K. Rostamzadeh, H. Nicanfar, N. Torabi, S. Gopalakrishnan, and V.C.M. Leung, "A context-aware trust-based information dissemination framework for vehicular networks", *IEEE Internet of Things journal*, Vol. 2, No. 2, pp. 121-132, 2015.

[16] N. Kumar and N. Chilamkurti, "Collaborative trust aware intelligent intrusion detection in VANETs", *Computers & Electrical Engineering*, Vol. 40, No. 6, pp. 1981-1996, 2014.

[17] M. H. Eiza, T. Owens, and Q. Ni, "Secure and robust multi-constrained QoS aware routing algorithm for VANETs", *IEEE Transactions on Dependable and Secure Computing*, Vol. 13, No. 1, pp. 32-45, 2015.

[18] R. Hussain, Z. Rezaeifar, Y. H. Lee, and H. Oh, "Secure and privacy-aware traffic information as a service in VANET-based clouds", *Pervasive and Mobile Computing*, Vol. 24, No. 1, pp. 194-209, 2015.

[19] S. Ahmed, M. U. Rehman, A. Ishtiaq, S. Khan, A. Ali, and S. Begum, "VANSec: Attack-resistant VANET security algorithm in terms of trust computation error and normalized routing overhead", *Journal of Sensors*, Vol. 2018, No. 1, pp. 1-17, 2018.

[20] P. Yang, L. Deng, J. Yang, and J. Yan, "SASMF: Socially Aware Security Message Forwarding Mechanism in VANETs", *Mobile Networks and Applications*, pp. 1-12, 2019.

[21] H. Xia, S. S. Zhang, B. X. Li, L. Li, and X. G. Cheng, "Towards a novel trust-based multicast routing for VANETs", *Security and Communication Networks*, Vol. 2018, No. 1, pp. 1-12, 2018.

[22] H. Hasrouny, A. E. Samhat, C. Bassil, and A. Laouiti, "Trust model for secure group leader-based communications in VANET", *Wireless Networks*, Vol. 24, No. 1, pp. 1-23, 2018.

[23] F. Goudarzi, H. Asgari, and H. S. Al-Raweshidy, "Traffic-aware VANET routing for city environments-A protocol based on ant colony optimization", *IEEE Systems Journal*, Vol. 13, No. 1, pp. 571-581, 2018.

[24] V. Krundyshev, M. Kalinin, and P. Zegzhda, "Artificial swarm algorithm for VANET protection against routing attacks", In: *Proc. of*

2018 IEEE Industrial Cyber-Physical Systems (ICPS), pp. 795-800, 2018.

[25] R. Sugumar, A. Rengarajan, and C. Jayakumar, "Trust based authentication technique for cluster based vehicular ad hoc networks (VANET)", *Wireless Networks*, Vol. 24, No. 2, pp. 373-382, 2018.

[26] V. Jain, R. S. Kushwah, and R. S. Tomar, "Named Data Network Using Trust Function for Securing Vehicular Ad Hoc Network", In: *Proc. Soft Computing: Theories and Applications*, pp. 463-471, 2019.