SECURE AND TRUSTABLE ROUTING PROTOCOL FOR ROUTING IN VEHICULAR DELAY TOLERANT NETWORK

Sana Abouljam[1*], Fathi A Hamhoum[3], Abdalla Mohamed Alasoud[2], Muner Athaba[1]

[1]*Compter Science Department, Faculty of Science – Ajaylat, University of Zawia*
[2]*Computer Department, Faculty of Science, Al-Asmarya Islamic University*
[3]*Compter Science Department, Faculty of Science – Zawia, University of Zawia*
[*]*Corresponding author: s.abouljam@zu.edu.ly*

ABSTRACT

Vehicle adaptive network (VANET) is an emerging field of wireless networking and one of the most promising applications for vehicle communication. In particular, many moving vehicles that do not have a pre-existing communication infrastructure are currently under increasing research interest to improve road safety. To provide reliable services, many challenges in VANET must be improved. These challenges include routing and security algorithms. Due to high mobility and ever-changing infrastructure, VANET's stable and reliable routing is one of the major issues.

To overcome those discrepancies, this paper proposes Cluster-Based – Trustable Routing Protocol (CB-TRP). Clustering of the vehicles is done using Artificial Neural Network, which considers the reliability rate value, speed, and distance difference among the nodes in the cluster formation. Also, routing is established using Trustable Routing Protocol (TRP). Finally, the privacy of the transmitted data is preserved using the K-anonymization method. Experimental results demonstrate the superiority and the effectiveness of the proposed system.

Keywords: Artificial Neural Network, Clustering, Cluster Formation, Trustable Routing Protocol, Vehicular Ad-hoc Network

1. INTRODUCTION

Recent network communication models usually support end-to-end communication. Rural discrete communications, "pocket switch networks", vehicle networks, and self-regulating networks are all examples of challenging non-traditional network environments characterized by unreliable resources and intermittent connections. Fault-tolerant network delay (DTN) tries to provide networking in these challenging environments [1]. Following (DTN) emerged as a communication solution in challenging environments such as deep space communications, private vehicle networks (VANETs), disaster recovery networks, and underwater networks, a new type of ad hoc network has emerged. It is believed that the Vehicle Delay Network (DTN) can be tolerated. The traditional ad hoc network adopts end-to-end communication from the source node to the destination node, but VDTN does not [2]. In a DTN, a message can be sent inside a path (also called a data packet) over an existing link and stored temporarily in the next step until the next link appears in the path (for example, a new node moves within a domain or an existing node wakes). This message delivery process is often referred to as a 'storage and paging' strategy and is directed in an 'opportunistic' manner [3].

In a vehicle network (VANET), continuous communication between vehicle nodes cannot be guaranteed everywhere. When the network presents rare transmission opportunities and intermittent connections, it is difficult for the vehicle node to forward the message to the destination. Delay and Disruption-Tolerant Networks (DTNs), implementing a “store, carry and forward” paradigm, are designed to operate under such conditions [4]. Therefore, most of the applications are based on the idea of Delay- and Disruption-Tolerant Networks (DTNs), where a packet in the network will be sent over an existing link and buffered at a node until a connection to a suitable next hop is established [5]. These networks are described by having intermittent connectivity, asymmetric data rates, long or variable delays, and high error rates [12]. Inability to guarantee proper security insurance when utilizing cloud administrations could at last result in higher expenses and potential loss of business, in this way taking out any of the potential advantages of cloud figuring [11]. Vehicular networks are formed by vehicles and fixed equipment situated at the margins of streets and highways. Vehicular Disruption Tolerant Networks (VDTN) aims to make available new technologies and applications, which can increase safety in streets and avenues through communication between users [6].

In recent years, delay-tolerance networks (DTN), such as satellite communications, networks in sparsely populated areas, and vehicle networks, have been extensively studied [7]. Delay tolerant networks (DTNs) have been recently increasingly applied to the applications such as distributed mobile healthcare systems and vehicular ad hoc networks (VANETs), where a contemporaneous end-to-end connection cannot be guaranteed [8]. Since a contemporaneous end-to-end path may never exist in DTNs, effective communication in DTNs requires the cooperation of all the nodes for routing and forwarding, where, the intermediate nodes on a communication path are expected to store, carry and forward the packets in an opportunistic way [7]. Privacy in Vehicular DTN (VDTN) is focused on the protection of the user/vehicular identity and the key idea is to use anonymity-based approaches. With the increasing deployments of satellites, traffic and surveillance video cameras, and all types of sensors and emerging services such as Google Earth, it becomes harder and harder to protect user privacy [9]. The secure routing technologies of mobile ad hoc networks cannot be fully applied to the VANET, so how to efficiently design security and trust mechanisms in the routing process is needed in VANET [10].

The draft structure of the paper is systematized as follows: Section 2 surveys the associated works regarding the proposed method. In section 3, a brief discussion about the proposed methodology is presented, section 4 analysis the Investigational outcome, and section 5 concludes the paper.

2. LITERATURE SURVEY

Lei Zhang et. al [13] proposed an advanced framework for opportunistic routing schemes, provided the following properties: the confidentiality of nodes' routing metric, anonymous authentication, and an efficient key agreement for pair-wise communication. Without the topology information and route maintenance processes, routing decision in opportunistic routing was made by exchanging and comparing the routing metrics among individuals, i.e., nodes with larger routing metric values were chosen as the relays. Under such a scenario, any one-hop routing followed the protocol flow that was proposed. Anonymous authentication was mainly provided in Sign and Verify algorithms. Experimental results showed that the security framework increased the original message size, leading to a larger overhead. For the same message size with a larger message generation interval, fewer messages were generated in the network, leading to lower resource competition and less overhead. A comprehensive assessment, including safety analysis, capabilities analysis, and simulation assessment is provided to demonstrate the safety and feasibility of the proposed framework.

Honglong Chen et. al [14] proposed a credit-based rewarding scheme called Earliest Path Singular Rewarding (EPSR) scheme to motivate the nodes to truthfully forward the messages during every contact opportunity. After that, they proposed another credit-based rewarding scheme called the Earliest Path Cumulative Rewarding (EPCR) scheme by further considering that a node may get more contact information from others. They proved that the proposed rewarding schemes were incentive-compatible, which guaranteed that the dominant strategy for the nodes was to truthfully forward the messages. It was also proved that the payment for each delivered message was upper bounded, making the proposed rewarding schemes applicable for the scenario when the nodes have a finite budget. Furthermore, the proposed rewarding schemes were resistant to the malicious behaviors of the selfish nodes. They conducted the simulations based on the real trace to illustrate the effectiveness of the proposed rewarding schemes.

Wu Qiwu et. al [15] proposed a new trusted routing protocol in VANET based on GeoDTN+Nav by using the trust management model of Bayesian and the three opportunistic routing forwarding models, the situation includes four steps to configure path, discover the path, create a trusted path, and delete the path. The proposed protocol not only improves routing security but also reduces time complexity. In the GeoDTN+Nav protocol, each vehicle was equipped with a virtual navigation interface (VNI). VNI was a lightweight package interactive interface with underlying vehicle components, which was to find the adjacent vehicles and provide the navigation interaction information with a consistent format. Most of the messages required for reputation management were realized in the original protocol extensions. Therefore, the proportion of the message payloads was acceptable to improve routing security. Experimental results and analysis showed that the protocol had achieved good performance in the removal ratio of malicious nodes, correct reception ratio of a packet, and the message payload.

Ying Cai et. al [16] presented an efficient incentive-compatible routing protocol (ICRP) with multiple copies for two-hop DTNs based on the algorithmic game theory. The potential for confrontation and the cost of dealing with the bad behavior of selfish contracts must be considered. Besides, they used the Best Stopping Rules Series and the Vickrey-Clarke-Groves Auction as a strategy to choose the best relay node to ensure that nodes that honestly report the odds and transmission costs they encounter can increase rewards. They attempted to find the optimal stopping time threshold adaptively based on a realistic probability model and proposed an algorithm to calculate the threshold. Based on that threshold, they proposed a new method to select relay nodes for multi-copy transmissions. To ensure the selected relay nodes can receive their rewards securely, they developed a signature scheme based on a bilinear map to prevent the malicious nodes from tampering. Through simulations, they demonstrated that ICRP can effectively stimulate nodes to forward/ carry messages and achieved a higher packet delivery ratio with lower transmission cost.

Suguo Du et. al [17] proposed a novel cooperative location privacy protection scheme, which was called AVATAR, for sparse DTNs. The main idea of AVATAR was to generate a certain number of virtual nodes in the proximity of a node and allowed both virtual and real nodes to make a coordinated pseudonym change in an enlarged region, which were named virtual mix zones. Each AVATAR participant benefited from increased location privacy protection at the cost of generating a series of signed position messages, which were named footprint signatures. To stimulate each node to contribute more footprint signatures to the virtual mix zones, AVATAR proposed a reward mechanism, which was modeled as a multiunit discriminatory auction game. The simulation result had verified the effectiveness of the AVATAR scheme. However, the current AVATAR scheme design in that paper was under the assumption of external attackers. For the case of internal attackers, which hold the real authorized credential from the OSM, AVATAR can still be secured when the requester can be trusted because a malicious AVATAR participant cannot link the old/private pseudonyms of the others.

Sulma Rashid et. al [18] presented a buffer scheduling policy called a weight based drop policy. In the proposed scheme, they dynamically adjust message weight parameters assuming message attributes. These features include message size, remaining time, the remaining time in the queue, number of hops, and number of iterations. To use the buffer effectively, they use the weighting criteria to find the most appropriate message, to ignore and arrange the messages sent to the nodes next to them. Simulated in a simulator. WBD reduces the load rate of the PRoPHET routing protocol. Overhead WBD was reduced by 60% compared to FIFO, 62% compared to MOFO, and 62% compared to DLA. Weight-based projection strategy simulation results using map-based navigation outperform current DLA, FIFO, MOFO, SHIL, and LIFO in terms of reducing transmission count, reducing messages and overheads, improving delivery, and average buffering time.

3. CLUSTER BASED – TRUSTABLE ROUTING PROTOCOL

Mostly, some selfish nodes in the compliant network like DTN could cause catastrophic destruction to any well-designed opportunistic routing jeopardize and scheme the complete network. This causes data confidentiality and identity verification issues as well as unique network security and privacy issues. To solve this selfish problem in DTN, we propose a block-based routing protocol (CB-TRP) technology. The compounds are assembled using an artificial neural network in a distributed manner taking into account the value of reliability rate, velocity, and distance difference between nodes in the formation of the block. These parameters increase connectivity and stability and can reduce network end-to-end bandwidth and delay. The cloud computing reliability of each vehicle depends on the characteristic parameters loaded by the corresponding vehicle. Also, according to the reliability provided by the cloud, vehicles in the network identify reliable forward nodes and complete the entire path. Finally, the K-anonymization method is used to securely transfer the transmitted data between nodes in the proposed protocol, and a schematic diagram of the method is shown in Fig.1.

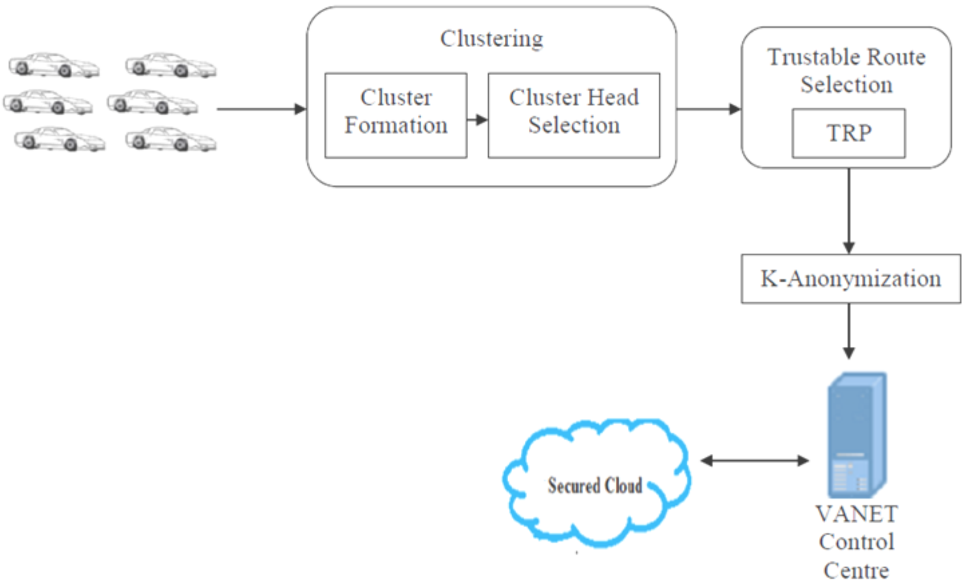

Figure 1: Overview of the proposed CB-TRP

3.1 Clustering

The proposed method is initialized with the clustering phase. In block-based routing, a group of nodes identifies themselves as being part of the block, and a node is designated as the head of the cluster that will broadcast the packet to the group. The steps involved in the clustering process are described as follows

- Cluster Formation.
- Cluster Leader Selection.
- Cluster Contract Certification.

3.1.1 Cluster Formation

To form a cluster, the proposed method utilizes the concept of Artificial Neural networks (ANN). Before proceeding to the formation of clusters, each node calculates its reliability rate value and then collects the information by its neighborhood to k-hops through the exchange of Hello message. Hello, the message contains information such as the identifier of the node, its status, its speed, and its reliability rate value. These parameters will allow creating clusters based on the method of ANN. Cluster Formation using ANN includes the following phases.

- Determining the reliability rate value.
- Determining the neighbor list.
- Forming clusters.

Determining the Reliability Rate Value:

Firstly, each vehicle calculates the reliability rate value (RRV) by the reputation score of each node based on its behavior. This score is calculated as the number of messages received by the number of the reply message

$$RRV = \frac{Number\ of\ \mathrm{Re}ceived\ Messages}{Number\ of\ Answered\ Messages} \times 100 \tag{1}$$

Determining the neighbor list:

A vehicle sends a "request" message in the network to collect information on the parameter table, and neighboring nodes respond with a "Hello" message containing: ID, speed, Current location (x, y), and the reliability rate value. After the exchange of Hello message with its neighbors, the vehicle calculates the distance among its neighbors using its neighbor list. The distance between the vehicle and its neighbor nodes by its location is given in equation 2.

$$D = \sqrt{(d_{xv} - d_{xn})^2 + (d_{yv} - d_{yn})^2} \quad (2)$$

The parameters such as speed, reliability rate value, and the difference in the distance are stored in an array $R[p]$.

Forming Clusters:

The proposed algorithm introduces a new ANN mechanism for the creation of clusters for reducing the number of messages exchanged among the neighbor vehicles. Artificial Neural Network incorporates a learning technique to predict the formation of clusters. During the process of cluster formation, ANN utilizes the information $R[p]$ of each vehicle, which depicts the information such as ID, speed, reliability rate value, and distance between a vehicle and its neighboring nodes. Figure 2 illustrates the schema of ANN.

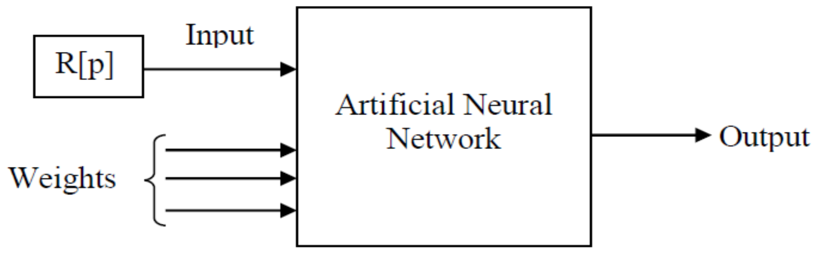

Figure 2: Schema of ANN

3.1.2 Cluster Leader Selection

After the cluster formation, the Cluster Head (CH) for each cluster is selected; the cluster-head is the node with the maximum degree of membership.

$$Cluster\ Head = Max(Degree\ of\ Membership) \qquad (3)$$

After the elected CH, CH broadcasts its new status to all members of clusters and its neighbors by sending a Hello message containing its ID and indicating a link among the members of its cluster. Each new member must inform the CH of its cluster by sending an affiliation message. Thus, the node becomes a member of this cluster and built its neighborhood table.

3.1.3 Cluster Contract Certification

`The identity verification process is described as follows: Instead of individually checking each node, the person in charge of the group gets information about every vehicle in the group and creates a batch file. The cluster sends the batch file to RSU for authentication. RSU forwards the file to the Local Sector Unit (LSU). LSU then extracts the information and verifies the identity of each vehicle of that batch. After successful verification, LSU issues an evidence token to the cluster leader. This token is an authentication certificate consisting of the cluster head's public key and its identification information to verify its authenticity to leaders of other clusters. In case of unsuccessful verification of a vehicle, LSU issues a warning to the vehicle's cluster leader by assigning a token meant for fraudulent vehicles. LSU communicates the information about the fraud vehicle to respective authorities for necessary actions.

3.2 Trustable Route Selection

To select a trustable path, a novel protocol named Trustable Route Protocol (TRP) is proposed. The proposed TRP utilizes the cloud sever to evaluate the trustworthiness of every vehicle in the network. The trustworthiness is given by the cloud based on attribute parameters (APs) uploaded by vehicles themselves. Nodes select an appropriate route by choosing an optimal relay node according to the trustworthiness of every candidate node. These candidate nodes are determined in the view of transmission probability. The protocol is composed of three phases.

- Preparatory phase
- Routing phase
- Delivery phase

Preparatory Phase:

In the preparatory phase, vehicles in the network upload attribute parameters of themselves collected by various sensors in vehicles. These parameters include the model of the vehicle, mileage, fuel consumption, vehicle accident records, violations of traffic regulations, and the number of times that the node acts as a relay node and the performance of the node. For instance, vehicles always have similar quality if they are the same model. Besides, the mileage and time of travel can reflect the frequency of vehicle utilization. An attribute parameter named anti-pheromone is also designed to create a more utilization efficient network, which is assigned for the Cluster Head (CH). In simple terms, the anti-pheromone is used to record the number of times each vehicle node in a cluster serves as a relay node and those values are maintained by the CH of that particular cluster. The cloud stores all the AP lists preparing for the trustworthiness evaluation.

Routing Phase:

In the routing phase, a node wants to transmit its message to a certain destination node. The node chooses a set of messages to the destination node. In the proposed TRP, the transmission probability is utilized to choose candidate nodes for the delivery phase. The value of transmission probability is evaluated by the positions of target nodes by using equations (4) and (5).

$$\Pr_{1\to 2}^{t} = \frac{S}{\pi R_{mov}^{2}} \tag{4}$$

$$\Pr_{1\to 2}^{t} = \frac{S}{2\pi}\left[\frac{R_{trans}^{2}}{R_{mov}^{2}}(\theta_1 - Sin\,\theta_1) + (\theta_2 - Sin\,\theta_2)\right] \tag{5}$$

If there are more nodes around the source node, the total probability is required to be calculated by using the equation (6).

$$\Pr_{1\to\forall}^{t} = 1 - \prod_{i=1}^{c}(1 - \Pr_{1\to i}^{t}) \tag{6}$$

The node that wants to deliver the message masters a list based on the range of acceptable transmission probabilities that should be set in advance. A candidate node list C contains the ID numbers of all nodes whose transmission probabilities satisfy the transmission requirement. This list contains all the nodes that have the chance to be chosen as a relay node. The candidate node list C should be sent to the cloud by the node who wants to know their trustworthiness and this node is named as the query node.

Delivery Phase:

When the query node wants to select an appropriate node in candidates to be the relay node, he sends the candidate node list to the cloud. The cloud will search the cloud storage to find out the up-to-date trustworthiness τ of the nodes in the list. The cloud will not directly send the trustworthiness value τ back to the query node. To prevent a too old trustworthiness value, the cloud will compare the timestamp of the trustworthiness with the timestamp of the query. If the trustworthiness is not fresh enough, the cloud will re-evaluate the vehicle. When the query node receives a trustworthiness list E, it performs the algorithm given in figure 3 to select the node that is the most suitable to be the next hop. Figure 3 shows the algorithm for selecting the trustworthy node to be the next hop.

```
E ← Trustworthiness evaluation values of the vehicles
provided by the cloud
m ← Selection of the relay node
t_m ← 0
while m do
        e ← one of the nodes in E
        E ← E − e
        T ← Timestamp of e
        if t ≻ t_m then
                t_m ← t
                t_m ← e
        else
                return
        end if
end while
return m
```

Figure 3: Pseudocode for trustworthy node selection for next hop

Figure 3, E is the record of the trustworthiness of candidate nodes provided by the cloud. The algorithm aims to choose the node with the largest trustworthiness value in the candidate node list.

3.2.1 Trustworthiness Evaluation

In TRP protocol, the Principal Component Analysis (PCA) approach is utilized to evaluate the vehicle trustworthiness τ according to the uploaded AP list which is a multivariable data table.

Standardization of the attributes:

A standardized index of each of the vehicles based on the h valid attribute parameters is calculated using the equation (7).

$$\bar{x}_{ij} = \frac{x_{ij} - \mu_j}{s_j},\ i = 1,2,...,h \qquad (7)$$

Where x_{ij} is the value of the j^{th} index of the i^{th} evaluation object? $\bar{x}_{ij}$ is the standardized value of x_{ij} .

$$\mu_j = \frac{1}{n}\sum_{i=1}^{n} x_{ij} \qquad (8)$$

$$s_j = \frac{1}{n-1}\sum_{i=1}^{n}(x_{ij} - \mu_j)^2 \qquad (9)$$

Correlation Coefficient Matrix:

The correlation coefficient matrix R is calculated according to vehicles and attributes parameters. The correlation coefficient matrix can be calculated by using equation 10.

$$r_{ij} = \frac{\sum_{k=1}^{n} \bar{x}_{ki} . \bar{x}_{kj}}{n-1}, (i, j =,2,..., m) \quad (10)$$

r_{ij} is the correlation coefficient of the i^{th} index and the j^{th} index.

Principal Components:

The principal component y_z in which z varies from1 to h is calculated using equation (11).

$$y_h = u_{1h}\bar{x}_1 + u_{2h}\bar{x}_2 + ... + u_{hh}\bar{x}_h \quad (11)$$

Contribution Rate Calculation:

The contribution rate of each principal component is calculated by using the equation (12).

$$b_j = \frac{\lambda_j}{\sum_{k=1}^{m} \lambda_k}, \; j = 1,2,...., m \quad (12)$$

According to the principal components, the trustworthiness evaluation can be done to make a comprehensive analysis of the corresponding vehicle.

Trustworthiness Calculation:

The trustworthiness value τ queried by the nodes in the network can be obtained by using the equation (13).

$$\tau = \sum_{j=1}^{p} b_j y_j \quad (13)$$

Where b_j is the information contribution rate of the j^{th} principal component

3.3 Securing using K-anonymization

The packets are initiated for transferring through the K-anonymization method. The trusted paths selected for packet transferring sends packets by securing the packet through the k-anonymization method which avoids the loss of data.

K-anonymity is the simplest form of the Anonymization method. It is the simplest implementation of the Anonymization method. A data set is called k-anonymized for any row with given attributes (fields) if there are at least $k-1$other data records that match the attributes. Two techniques are used to implement k-anonymity. The first is sovereignty and the second is a generalization. In Supersession, some key attributes are replaced by some notation, such as `` * " or some static values (such as 0). For example, if Supersession is applied, "name" in the table is a major attribute, and age is a semi-identifiable attribute. Change it to "Name" and use the "*" symbol instead. "*" As another table, you can hide basic information from the database. Here, the data sent between nodes in the proposed privacy protocol is sent in a secure manner using K anonymization.

4. RESULT AND DISCUSSION

Our proposed methodology is employed in the JAVA platform with machine configuration of processor type Intel core i3, OS type should belong to Windows 7 having the CPU speed of 3.20 GHz and the memory of RAM can be distinguished as 4GB. JAVA is a general purpose programming language, which produces software for multiple platforms with a vast number of features. Java can be used to create complete applications that may run on a single computer or be distributed among servers and clients in a network. In our simulation, total n DTN vehicular nodes with a transmission radius of 300 meters are uniformly deployed in an area of $6000\text{m} \times 10000\text{m}$ and the shortest path map based movement routing is selected since the message is forwarded by the vehicles moving along the streets.

4.1 Performance Analysis

In this section, the performances are analyzed using existing methods and compared with the proposed method. Our key effort is examining the performance of the intended effort and monitors how it varies with few other conventional methods for cloud based vehicular networks.

4.1.1 Performance Analysis on Clustering

The performance of the proposed algorithm for clustering that is based on the Artificial Neural Network (ANN) was compared with the clustering technique used in the existing Trust-Based VANET Network (TBVN).

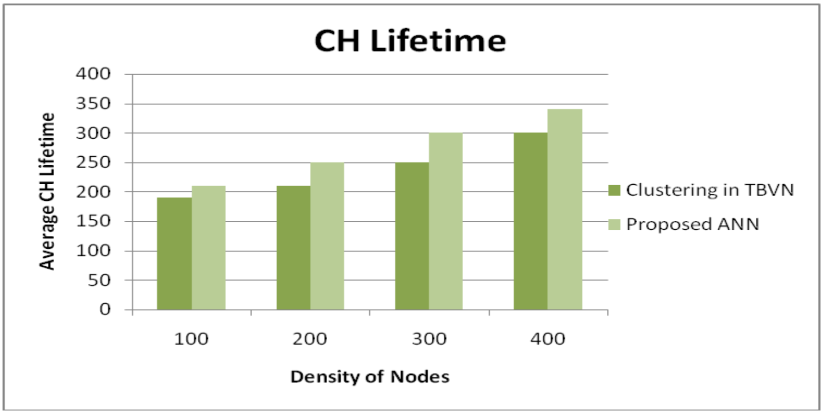

Figure 4: Comparison of CH Lifetime

Figure 4 depicts the variation of the average CH lifetime compared to the vehicle density. By increasing the number of vehicles, the number of CH will decrease. Therefore, the average CH lifetime will increase. Moreover, by decreasing the number of cluster-heads, the probability of a member leaving the old cluster and joining a new cluster decreases. Consequently, it can be seen that the performance of the proposed approach is a clear improvement when compared with the existing clustering technique TBVN.

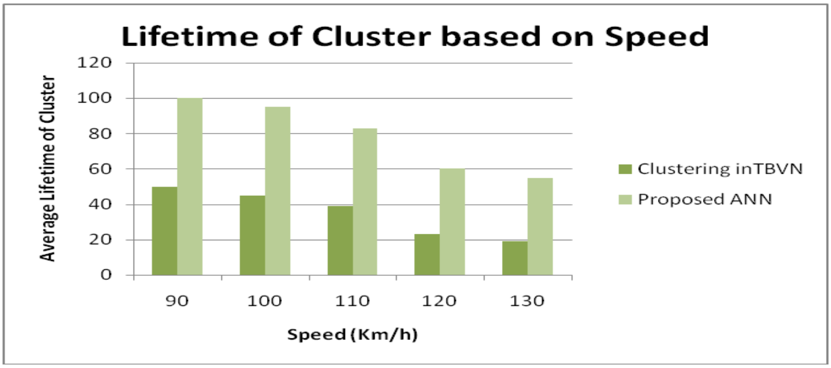

Figure 5: Comparison of Clusters' Lifetime

Figure 5 depicts the lifetime of the clusters when done with the existing clustering in TBVN and the proposed ANN for clustering. Since when the vehicle moves faster the topology of the vehicle network is more dynamic, the average CH lifetime and the average lifetime of the cluster will decrease when the speed of vehicles increases. It can be inferred that the proposed ANN clustering technique is superior to the existing one in terms of clusters' lifetime.

4.1.2 Performance Analysis on Trust based Routing

This section analyses the performance of the proposed Trustable Routing Protocol (TRP) and it is compared with the existing Trust Based VANET Network (TBVN).

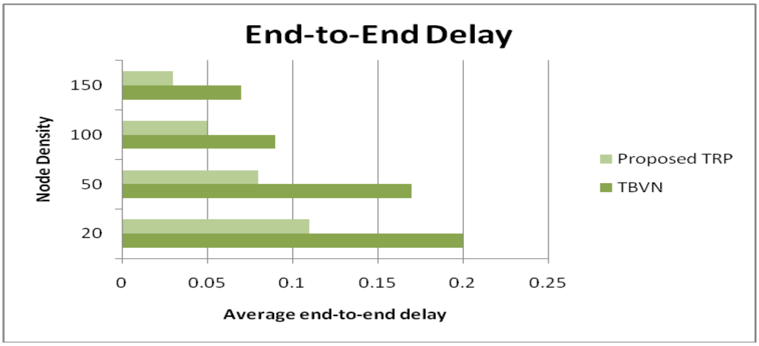

Figure 6: Comparison of end-to-end delay

Figure 6 analyses the end-to-end delay of the existing TBVN and the proposed TRP protocol. TRP can obtain a smaller delay because, with the help of the cloud, the node can determine the next hop node more quickly. As the node density increases, the average end-to-end delay decreases and it can be inferred from figure 6 that there is a large variation when comparing the existing and the proposed method.

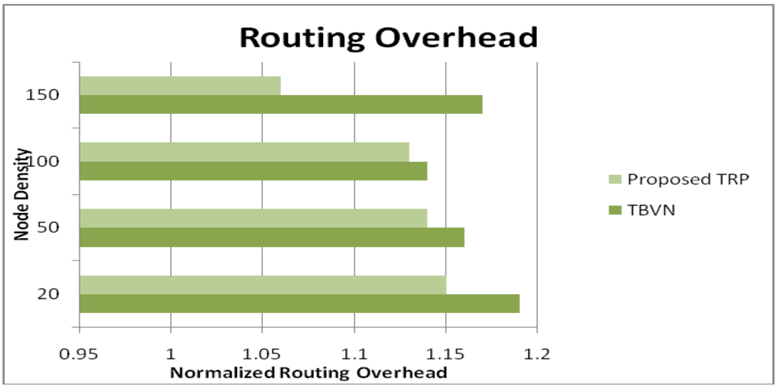

Figure 7: Comparison of Routing Overhead

Figure 7 analyses the routing overhead of the existing TBVN and the proposed TRP protocol. The TERP only requires the cloud to give a reasonable value of trustworthiness, which reduces the abuse of broadcast packets and the frequency of use of nodes. So, the overhead in the network has been reduced.

4.2 Overall Performance of the Proposed Method

Overall performance of the proposed method Cluster-Based – Trustable Routing Protocol (CB-TRP) is compared with the existing TBVN in terms of Packet Delivery Ratio and Computational Time.

4.2.1 Packet Delivery Ratio

The transmission rate of data packets is the ratio of the number of data packets a target receives to the number of data packets sent by the sender. This is the most important indicator we should keep in mind when forwarding packets. It may be affected by many key factors such as package size, team size, the scope of work, and contract changes. Strong messaging is defined as 100% packet data delivery. Here, 100% delivery means that the recipient receives all packages sent by the sender node before the period expires. The delivery ratio can be given by the equation (14).

$$Delivery\ ratio(d) = \frac{No.of Packet\ \mathrm{Re}ceived\ by\ the\ Destination}{No.of\ Packet\ Sent\ by\ the\ Sender} \tag{14}$$

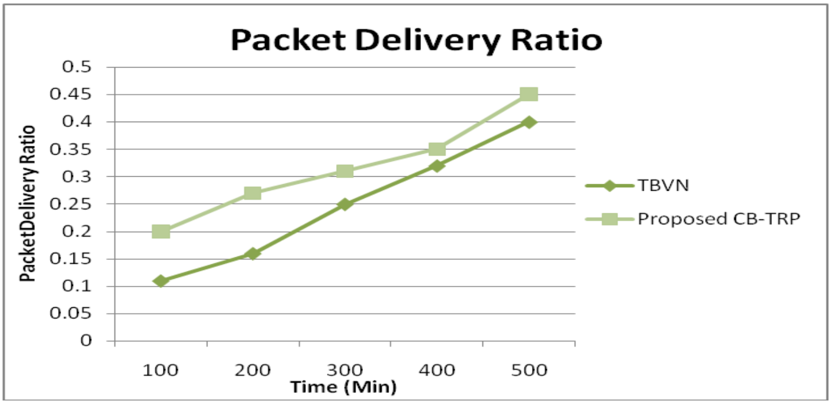

Figure 8: Comparison of Packet Delivery Ratio

Figure 8 gives the comparison of the proposed CB-TRP with the existing method TBVN in terms of packet delivery ratio. From the graph, it is observed that the curve plotted for the proposed CB-TRP goes in a rising manner which indicates that the delivery ratio of the intended CB-TRP is high compared to that of the existing method. The larger the delivery ratio is, the more vehicles are willing to forward packets. The higher the value of the delivery ratio the chance of packet loss is minimized which shows the better performance of the intended CB-TRP.

4.2.2 Computation Time

Generally, evaluation of the computational time is vital for assessing the performance of any system. The time of computation for any system must be minimized so that the system is said to have a good performance. The comparison of computational time of the proposed CB-TRP with the existing method TBVN is shown in figure 9.

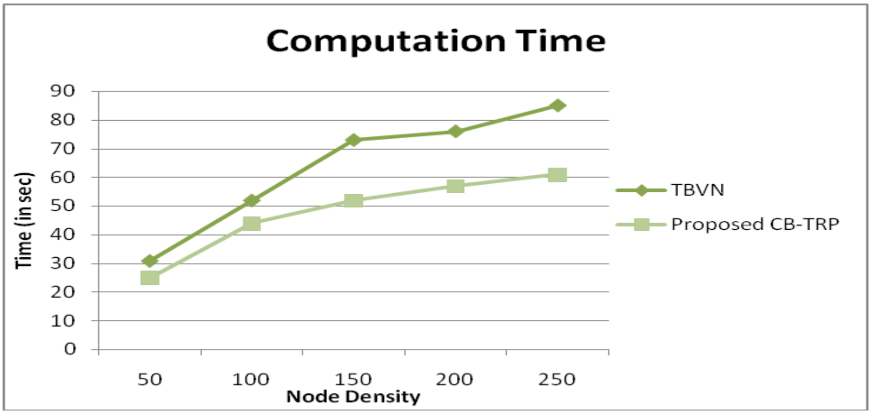

Figure 9: Comparison of Computation Time

Figure 9 gives the comparison of the proposed CB-TRP with the existing method TBVN in terms of computation time. The computation time of the existing TBVN is too high and it increases as the node density increases. It can be inferred that the time for computation is low in the case of the proposed CB-TRP when compared to the existing TBVN.

5. CONCLUSION

This paper proposes a novel Cluster Based – Trustable Routing Protocol (CB-TRP) technique, in which clustering is done based on the Artificial Neural Network approach and trustable routing is done using Trustable Routing Protocol. The results were analyzed to demonstrate the performance of the proposed method with another existing method. From the observation of the evaluation metric values, we can assume that our proposed technique will outperform better than any other techniques by having better evaluation metrics. The proposed protocol CB-TRP finds the trusted path of all available nodes to calculate the trust values of each request. Thus the data is transferred securely. Finally, the security analysis and the extensive simulations demonstrate the effectiveness and practicability of our proposed CB-TRP.

REFERENCES

[1] Rob Jansen, and Robert Beverly, "Toward anonymity in delay tolerant networks: threshold pivot scheme", In MILITARY COMMUNICATIONS CONFERENCE, 2010-MILCOM 2010, pp. 587-592, IEEE, 2010.

[2] Chibueze P. Anyigor Ogah, Haitham Cruickshank, Zhili Sun, Ganesh Chandrasekaran, Yue Cao, Philip Michael Asuquo and Masoud Al Tawqi, "Privacy-enhanced group communication for vehicular delay-tolerant networks", In Next Generation Mobile Applications, Services and Technologies, 2015 9th International Conference on, pp. 193-198, IEEE, 2015.

[3] Haojin Zhu, Xiaodong Lin, Rongxing Lu, Yanfei Fan, and Xuemin Shen, "Smart: A secure multilayer credit-based incentive scheme for delay-tolerant networks", IEEE Transactions on Vehicular Technology Vol. 58, No. 8, pp. 4628-4639, 2009.

[4] Yinghui Guo, Sebastian Schildt, Tobias Pogel, and Lars Wolf, "Detecting malicious behavior in a Vehicular DTN for public transportation", In Global Information Infrastructure Symposium, 2013, pp. 1-8, IEEE, 2013.

[5] Yinghui Guo, Sebastian Schildt, Tobias Po, Stephan Rottmann, and Lars Wolf, "Mitigating blackhole attacks in a hybrid VDTN", In World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2014 IEEE 15th International Symposium on a pp. 1-6, IEEE, 2014.

[6] Thiago Rodrigues de Oliveira, Sérgio de Oliveira, Daniel Fernandes Macedo, and José Marcos Nogueira, "Social networks for certification in vehicular disruption tolerant networks", In Wireless and Mobile Computing, Networking and Communications (WiMob), 2014 IEEE 10th International Conference on, pp. 479-486, IEEE, 2014.

[7] Rongxing Lu, Xiaodong Lin, and Xuemin Shen, "Spring: A social-based privacy-preserving packet forwarding protocol for vehicular delay-tolerant networks", In INFOCOM, 2010 Proceedings IEEE, pp. 1-9, IEEE, 2010.

[8] Jun Zhou, Xiaolei Dong, Zhenfu Cao, and Athanasios V. Vasilakos, "Secure and privacy-preserving protocol for cloud-based vehicular DTNs", IEEE Transactions on Information Forensics and Security Vol. 10, No. 6, pp. 1299-1314, 2015.

[9] Carson Dunbar and Gang Qu, "A DTN routing protocol for vehicle location information protection", In Military Communications Conference (MILCOM), 2014 IEEE, pp. 94-100, IEEE, 2014.

[10] Qiwu Wu and Qingzi Liu, "A trusted routing protocol based on Bayesian in VANET", International Conference on Cyberspace Technology (CCT 2014), 2014 page 026 (4) 2014.

[11] S. Anu Ranjana, CL Stefi Sterlin, W. V. Benita, and B. Baron Sam. "Secure and concealment in the cluster-based framework on vehicular networks." In Information Communication and Embedded Systems (ICICES), 2017 International Conference on, pp. 1-6, IEEE, 2017.

[12] Milind R. Penurkar and Umesh A. Deshpande, "OPPRES: Opportunistic Routing algorithm for routing messages in emergencies using vehicular delay-tolerant network", In Advanced Networks and Telecommunications Systems (ANTS), 2016 IEEE International Conference on, pp. 1-6, IEEE, 2016.

[13] Lei Zhang, Jun Song, and Jianping Pan, "A Privacy-Preserving and Secure Framework for Opportunistic Routing in DTNs", IEEE Transactions on Vehicular Technology Vol. 65, No. 9, pp. 7684-7697, 2016.

[14] Honglong Chen, Wei Lou, Zhibo Wang, and Qian Wang, "A secure credit-based incentive mechanism for message forwarding in noncooperative DTNs", IEEE Transactions on Vehicular Technology Vol. 65, No. 8, pp. 6377-6388, 2016.

[15] Wu Qiwu, Liu Qingzi, Zhang Long, and Zhang Zhiming, "A trusted routing protocol based on GeoDTN+ Nav in VANET", China Communications Vol. 11, No. 14, pp. 166-174, 2014.

[16] Ying Cai, Yanfang Fan, and Ding Wen, "An incentive-compatible routing protocol for two-hop delay-tolerant networks", IEEE Transactions on Vehicular Technology Vol. 65, No. 1, (2016): 266-277.

[17] Suguo Du, Haojin Zhu, Xiaolong Li, Kaoru Ota, and Mianxiong Dong, "MixZone in motion: achieving dynamically cooperative location privacy protection in delay-tolerant networks", IEEE Transactions on Vehicular Technology Vol. 62, No. 9, pp. 4565-4575, 2013.

[18] Sulma Rashid, Qaisar Ayub, and Abdul Hanan Abdullah, "Reactive weight-based buffer management policy for DTN routing protocols", Wireless Personal Communications Vol. 80, No. 3, pp. 993-1010, 2015.