International Journal of Engineering & Technology, 7 (1.1) (2018) 199-205

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Cloud based secured privacy preserving protocol for vehicular DTNS

Sana Mohammed Abouljam [1] *, Tulika [2]

[1] *Computer Science and Information Technology*
[2] *Associate Professor, SHUATS University*
**Corresponding author E-mail: sana1984mohammed@gmail.com*

Abstract

In this work, our research focuses on a design for request distribution and associated security attacks in dense vehicular ad hoc networks (VANET) and also sparse VANET that creates a delay tolerant network (DTN). Generally vehicles are stratified into clusters; we presented a reliability based clustering which has been designed for VANET. Cluster creation is according to complicated clustering metric that considers density of relation graph, link value and also traffic conditions. Since the ones in specific time and location are always affecting with the similar pattern of the direction and also velocity. A vehicle communicates with other vehicles or it's nearest Road Side Unit (RSU), which provides an access for a local cloud for sending appeals. We define the formal security model k-anonymization of privacy preserving aggregated transmission evidence generation (ATEG) in our proposed trust based VANET network (TBVN). It is required that both the individual vehicle velocity and the average velocity of vehicle clusters should be well protected from the semi-trusted vehicular cloud and the malicious running vehicles. Therefore, except for the traditional security requirements such as data secrecy and authentication, unique safety and privacy concerns are emergently should be rectified.

Keywords: *Vehicular Ad Hoc Networks; Clusters; K-Anonymization; Aggregated Transmission Evidence Generation; Vehicular Cloud; Connection Graph.*

1. Introduction

Vehicular Cloud Computing is an innovative technological shifting, that utilizes cloud computing benefits for serving the VANETs drivers with pay while you move model (Whaiduzzaman, 2014).VANET (Vehicular Ad Hoc Network) has emerged from MANET (Mobile Ad Hoc Network) since its specialized breed by employing vehicles as nodes while the road topology restricts nodes mobility. VANET has inspected ample amount of researchers for providing consumers and drivers with reliable, safe and also infotainment-rich driving occurrence. Nonetheless, automobile companies have been yet reluctant for deploying VANET in a whole scale owing to the safety and also privacy challenges (Hussain, 2014). The developed applications for VANETs are stratified into three significant categories: 1) safety applications (for instance, road hazard control notification plus emergency electronic break light), 2) convenience applications (e.g., parking availability notification plus congested road notification,), and 3) commercial applications (e.g., service announcements plus content map database download) (Wang, 2016).

These applications create messages of two sorts for VANETS communications including safety and also non-safety messages. The safety messages comprising beacon and then exigency messages are relegated in the control channel. The relegation of non-safety messages containing the messages created by convenience and commercial applications is done in service channels. (Taherkhani, 2016). Matched with MANETs, vehicular networks possess some designated characteristics and also networking properties that include: predictable mobility model, large-scale networks, variable network density, and finally very rapid topology modifications (Louazani, 2014). The formation of VANET by vehicles is conjoined with wireless communication devices, digital maps and with positioning system. Also, it permits vehicles for connecting to roadside unit (RSU), fixed infrastructure utilizing dynamic computing devices (Whaiduzzaman, 2014). Therefore, vehicle-to-vehicle and then vehicle-to-infrastructure communication will be practicable. Vehicular ad hoc networks are used for an expansive array of safety applications (Singh, 2015) (collision warnings with traffic information) also non-safety applications (like road navigation and also mobile infotainment). Owing to the practicability of accidents and also life-critical situations, the safe information exchange amidst vehicles is significant (Lu, 2016) (Mandal, 2014). One of the basic challenges is the privacy perpetuating authentication of a vehicle. The mechanism must provide some methods for pursuing a user in a malicious activity case detection. (Rajput, 2016). Other hand, privacy preservation should be effectuated in the sense where the user-based private information, that includes driver's name, speed ,license plate, position, and also traveling routes and finally their relationships must be protected (Cho, 2013). These privacy preserving schemes are widely categorized in the pseudonymous based schemes (Wang, 2016) (Jinyuan Sun, 2010) and (Chim, 2014) or the schemes based on group signature (Kaushik, Sapna, 2013) (Lin, 2013) (Zhang, 2014) the scheme based on Pseudonymous utilizes a pseudonym impertinent to the actual particularity of the senders with the purpose of preserving their seclusion in the communicating procedure. The scheme concerning Group-oriented signature is utilized widely in VANETs for the vehicles for achieving anonymous authentication, since it is competent of removing the inefficacy of the approach regarding Pseudonym (Wang, 2016).

VANETs enable vehicles for exchanging contemporary traffic information enhancing the traffic flow and also driving safety. If the information is altered or misstated with the user of a malicious vehicle, very serious consequences of traffic blockage and a traffic accident can also occur. Same time, the authorities must be able for revealing the identities of the message senders in the event of billing purpose for navigation services or tracing the compromised subscriber who can commence the denial-of-service attack for threatening the system (Cho, 2013). Delay tolerant networks (DTNs) have been presently increasingly utilized to the applications of distributed mobile healthcare systems and VANETs, while a contemporaneous end-to-end connection may not be guaranteed (Zhou, Jun, 2016). DTNs have greatly benefited for improving road safety and traffic efficiency. It mainly comprises the following unique characteristics. Firstly, though appropriately powered, Onboard Units (OBUs) storing private information for securing the communication in VANETs, equipped on the vehicles, are required generally for testifying about 1000-5000 messages per second with about 100-500 vehicles in the communication range and unable to afford computational tasks with heavy complexity, and tempted to suffer from sophisticated attacks and even node compromise attack.

2. Recent related researches: a review

Ubaidullah Rajput et.al (Rajput, 2016) have suggested an effective and also practical pseudonymous authentication protocol utilizing conditional privacy preservation. Their protocol suggests a pseudonyms hierarchy concerning the particular time duration of their utilization. They suggested the primary pseudonyms concept with comparatively longer time durations which were utilized for communicating with semi-trusted authorities and the secondary pseudonyms with lesser life time utilized for communicating with other vehicles. Their protocol only foresees an honest-but-very curious behavior from the fully credible authorities. Their protocol does not demand for conserving a CRL and inherent mechanism reassures the receiver that the corresponding pseudonym and the message are very safe and authentic. They completely investigated our protocol for exhibiting its resilience opposite to different attacks and presents computational and communicational overhead evaluation to present its robustness and efficiency.

SubirBiswaset.al (Biswas, 2013) they suggested an unspecified authentication and also verification technique for the IEEE Wireless Access in Vehicular Communications (WAVE)-related VANETs. Their involvement comprises Vehicular message confirmation and an efficacy strategy of prioritized verification for the periodic road security messages is included in their contribution. A deviation of elliptic curve digital signature algorithm (ECDSA) was utilized in amalgamation of the identity-based (i.e., ID-related) signature, in which present location facts on a vehicle was utilized like the ID of the associating vehicle. That waives the inevitability to a third-party open main certificate for VANETs message authentication. A peak-density road traffic circumstance forms a challenge to the vehicular messages authentication as the verification time required is frequently much longer than the approximate inter arrival time. To alleviate the issue, every traffic class messages are checked preceding the VANET's medium access control (MAC) layer precedence than the application appropriate of individual security messages.

Jinyuan Sun et.al (2010) have suggested a security system to VANETs for achieving privacy wanted by vehicles and also traceability demanded by authorities of law enforcement, Moreover, fulfilling basic security requisitions comprising authentication, message integrity, non-repudiation, and confidentiality. They suggested a privacy-preserving protection method for network authorities for handling mischief in accessing VANET, recognizing the challenge which privacy proffers avenue for mischief. The suggested system engages an identity-related cryptosystem in which certificates are not required for authentication. Also, they present the feasibility and also achievement of our system regarding the security aims and efficacy.

Neetesh Saxena et.al (2017) have suggested a scheme having the below security and also privacy-preserving components: anonymous authentication, anonymous signatures, fine-grained accessing control, information confidentiality, remote attestation, message integrity, and a payment structure. Here, that article was intended toward practitioners concerned in scheming and also implementing safety and privacy-conserving networks to smart V2G applications.

Internet access via public hotspots situated inside the public transportation methods, like trains, buses, and shuttles. Passengers within such public transportation systems experience complete Internet access utilizing variant MNNs, of cell phones and also personal digital assistants. And, because of the wireless network environments open nature, physical-layer attackers may easily find the MNNs computing the received signal strength (RSS) within the positioning schemes of triangulation scheme.

Sanaa Taha et.al (Taha Sanaa, 2013)they changed obfuscation, i.e., concealment, and power variability concepts and suggest an innovative physical-layer location privacy scheme, i.e., the false point–cluster-related scheme, for preventing the attackers from the users localizing within VANET hotspots based on NEMO. The presented scheme engages fake-point- acknowledged and sub schemes based on cluster, and its aim is to perplex the attackers by developing their RSSs measurements evaluation errors and, so, sustaining MNNs' location privacy.

Yaqoob et al. (2017) have analyzed contemporary leading research advances in SDVN paradigm. Next we stratify and categorize SDVN ideas and implement taxonomy according to significant characteristics, like services, network architectural components, access technologies, opportunities, system components and operational modes,. Moreover, they recognized and designed the main requisitions for SDVNs. Lastly; they calculated and outlined upcoming research challenges.

3. Proposed trust based vanet network

Generally few egotistical nodes of a cooperative network of DTN could cause catastrophic defection to any good modeled opportunistic routing methodology and jeopardize the complete network. This directs to the issue in data confidentiality, authentication, and distinctive safety and also privacy issues in the network. For addressing such sort of selfishness issue in DTNs we suggested the trust related VANET network. In this sector, we proffer an elaborated presentation of our suggested efficient privacy-preserving trust based VANET network which is regarding trust and reliability which comprises the below four phases:

- Clustering,
- Trust Calculation,
- Trust Based Path Selection and
- Securing utilizing K-anonymization

3.1. Clustering

The recommended methodology is commenced with the clustering phase. In cluster related routing an association of nodes recognizes themselves for being a part of cluster and also a node is chosen as cluster head and will transmit the packet to cluster. Here, the procedures associated in clustering procedure are illustrated as follows

3.1.1. Cluster formation
3.1.2. Cluster leader selection
3.1.3. Cluster nodes authentication

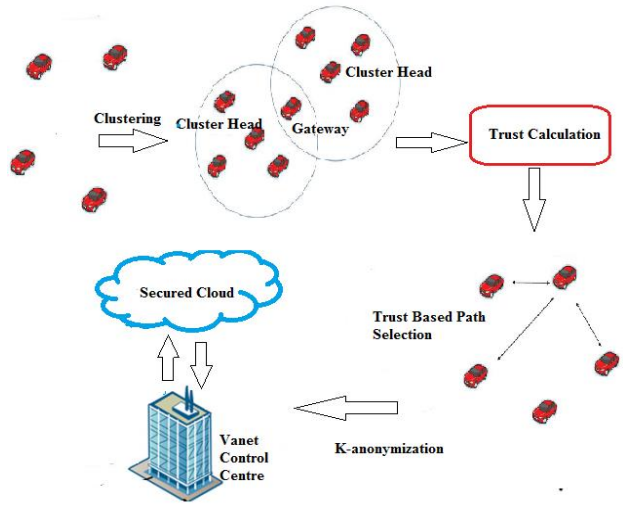

Fig. 1: Architecture of the Suggested Trust and Reliability Based Privacy Preserving Protocol.

3.1.1. Cluster formation

In the cluster creation phase, a cluster is formed with integrating the vehicles going in the similar direction. During cluster formation, divergent parameters of speed, direction of nodes and range betwixt farthest nodes are considered. RSUs continuously check vehicles for clustering. If there is an independent vehicle, RSU instructs OBU (On-board Unit) of that vehicle to get related with the customary nearby cluster. If there is more than one non-clustered vehicle, the first non-clustered vehicle is declared as the temporary leader of hypothetical cluster which initiates the clustering process. All vehicles gather the neighboring node's information such as speed, direction and calculate approximate distance between them. Temporary leader vehicle selects a median speed vehicle in its communication range. Further, the leader trains the selected vehicle to continue the clustering process. Afterwards, the newly selected vehicle is preferred as the temporary leader for further cluster formation. Finally, the temporary leader starts the clustering process by defining a cluster radius to ensure the participation of every vehicle in the array for clustering.

3.1.2. Cluster leader selection

The temporary leader selected in cluster creation phase initiates the cluster leader selection process. Mean square value of associated tempo of the vehicles in the cluster is measured through the temporary leader. The vehicle having the slightest mean square value of relative speed is chosen as the cluster leader. The benefit of using mean square method is that the selected leader will remain within the cluster for longer period. Nearest RSU can communicate the information about selected leader to CU. The history of cluster leaders is used for computing trust component. The mean square value of vehicle β is calculated using eq. 1. Here, X_i' represents the vehicle for which mean square value β is calculated and X_i represents other vehicle's speed in the cluster. The β is described by

$$\beta = \frac{1}{n}\sum_{i=1}^{n}(X_i' - X_i)^2 \quad (1)$$

3.1.3. Cluster node authentication

Authentication process is described as follows: Instead of every node authenticating itself, the cluster leader takes the information of each vehicle in that cluster 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 cluster leader. This token is an authentication certificate consisting of cluster head's public key and its identity information to verify its authenticity to leaders of other clusters. In an unsuccessful verification case of a vehicle, LSU issues a warning to the vehicle's cluster leader by assigning a token meant for fraud vehicles. LSU communicate the information regarding the fraud vehicle to respective authorities for necessary actions.

3.2. Trust calculation

The trust stage allotted to a node has been an integration of direct interaction having its neighbors and also the recommendations by its peers. A node allots a direct trust phase to its neighbor concerning the derived acknowledgements. When the neighbor sends a timely recognition of the received packet, it is presumed that the node has not related in a resource intensive brute-force attack .Therefore it is allotted to a greater trust level. Then the direct trust is integrated with the trust recommendation with its peers and a last trust level is allotted to it. Mention that such trust levels are dynamically assigned and are coached through a node to performance improvement. The trust commendations are piggy backed on DSR routing packets. Let Figure 2 be considered.

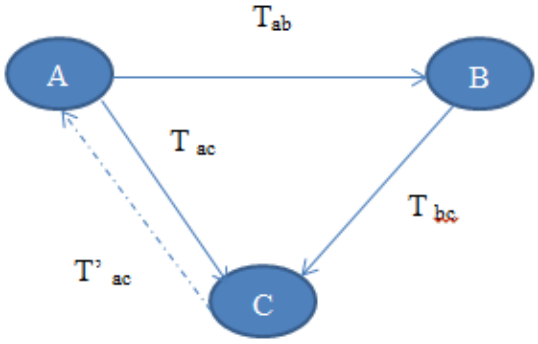

Fig. 2: Trust Assignment.

Let $T_r ab$ represents the straight trust in node B by node A and let $T_r bc$ represents the trust suggested by the node B in node C . If $T_r ac$ represents the direct trust of node C in node A , then the trust assigned by A in C is given as the mutual trust. The mutual trust is described by

$$T_r'xz = 1 - (1 - Tac)(1 - Tabc)\beta ; \quad (2)$$

Where

$$T_r abc = 1 - (1 - Tab)^{Tbc} . \quad (3)$$

The trust stages are normalized to integer values using standard methods. Every node is provided an integer trust value that lies betwixt 0 and 1. When an innovative node combines the network, it delivers a hello packet for its neighbors. Here, the neighbors may allot an original trust value of 0.5 to the node. Moreover, the trustworthiness in the node is augmented if the node presents generous behavior. Likewise, whilst the network is left by the node, it might not respond any more to the messages. The neighbor may wind up that the network has lost its connectivity or the node has exited the network. In such scenario, the network would delete the node from its network's table and would broadcast this information to other network nodes. These nodes would then delete this table from their route cache.

For computing path trust, the RREQ with RREP packets are customized thence they comprise the trust value in the node from where the packet is derived. Both packets are modified as in route discovery the node transfers the RREQ packet through broadcasting. A node acknowledges the node only from which the packet is acknowledged, not the node to which it must be transmitted. Thence, the RREQ packet is altered for integrating the former

node's trust value and the RREP packet is altered for integrating the following node's trust value.

3.3. Trust based path selection

The trust value measured with the trust methodology in the earlier procedure is utilized for choosing the trust related path. Amidst every possible path with computed trust value The path with the highest trust value is chosen in this technique.

Path trust has been the trust value related with the path. Such value is signified as the weighted average in the trust value of the nodes of the path. Trust is regarded to be asymmetric, hence mutual trust $T_r'xz$ betwixt the nodes x and also z is utilized. Also, Hop count has a significant part in the path selection as the huger the nodes number, more is the slowdown in the network and also the chances of information alteration also augments. The average in the trust values of the node in the path is computed for choosing the trusted path. The path with the highest average trust value is selected amidst the possible Pn paths. For instance let the mutual trust in nodes x and z which are accessible in initial path (P1) be $T_r'xz$ and also the mutual trust in nodes a and b be $T_r'ab$ that associate to the similar path (P1). Next the average trust value $T1_{avg}$ of the path 1 is measured through

$$T1_{avg} = \frac{T_r'xz + T_r'ab}{2} \quad (4)$$

Where $T_r'xz$ has been the mutual trust of nodes x and z

$T_r'ab$ is the mutual trust of nodes a and b

$T1_{avg}$ is the average trust of path P1

Similarly the average trust $T1_{avg}$ is computed for every available paths P_1.....P_n .The path with the highest trust average T_{avg} is chosen to data transfer. If $T1_{avg} > T2_{avg}$, next the path P1 is chosen for transferring the packet.

3.4. Securing using k-anonymization

The path with the highest trust value is chosen to packet transfer. The packets are initiated for transferring through the K-anonymization method. The trusted paths selected for the intent of packet transferring sends packet by securing the packet through the k-anonymization method which avoids the loss of data.

K-anonymity has been the easiest Anonymization method form. It is the easiest execution of Anonymization technique. A data set is termed k-anonymized to any row with provided attributes (fields) when there are even $k-1$ other data records which compare the attributes. Two methods are utilized for implementing k-anonymity. Original has been the Supersession and also the second has been the Generalization. Here, In Supersession few main quality is substituted with few symbols of'*' or else some constant values of 0. For instance in table "Name" has been Key attribute and also Age has been a quasi-identifier attribute, if Supersession is utilized to "Name" and substitute it through symbol '*' as another table , then main facts are concealed from database. Here the data provided betwixt the nodes in the suggested privacy conserving protocol is passed on in a secured manner utilizing such 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 intention programming language, which creates software for several platforms with vast number of features. Java is used to generate whole applications which might run on a solo computer or else be shared amidst servers and also clients in a network. In our replication, totally n DTN vehicular nodes having a transmission radius of 300 meters are deployed uniformly in an area of $6000m \times 10000m$ and the tiniest path map related movement routing is selected since the message is forwarded by the vehicles stirring along the streets. In this scenario, each vehicle randomly selects a destination and moves there for a2 min. pause, and then it repeats the above until the simulation is done.

We considered three datasets for our proposed work simulation which includes a simple urban vehicular traffic scenario in a 600 m × 1000 m bidirectional road with two lanes in every direction. The data set 1 is the street map view of BerlinCity, data set 2 is the street map view of New York city and data set 3 is the street map view of Puebla city. An RSU is implemented at the roadside, whereas different numbers of OBUs are mounted with moving vehicles on road.

4.1. Performance analysis

In this segment, the performances are analyzed using divergent methodologies and paralleled with the recommended methodology. Our key effort is examining the intended effort's performance and monitors how it varies with few other conventional methods for cloud based vehicular networks.

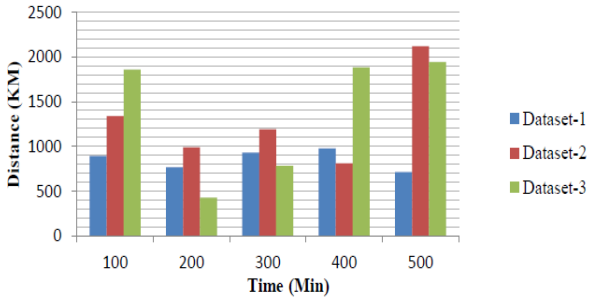

Fig. 3: Distance Travelled by Nodes in Various Dataset.

Discussion: The above noted figure describes the complete distance travelled by the vehicles for 3 different data sets of 3 different cities. For example initially for 100 minutes the three dataset of 3 cities is compared showing the total distance the vehicles travelled in that particular distance. Likewise the distance travelled for 200,300,400 and 500 minutes is compared for the available three datasets. The optimum distance covered in possible data set is about 2500 km.

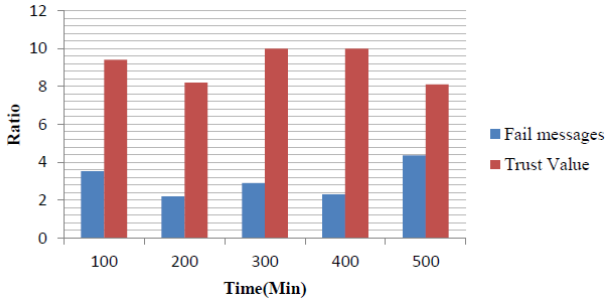

Fig. 4: Rate of Fail messages and trust values for the data set 1 using the proposed TBVN

Discussion: The above illustrated figure gives the rate of fail messages and trust values for the suggested TBVN method applied to the data set 1.From the above bar diagram it is noticed that the occurrence of the fail messages are very low which presents that the messages are delivered in a better manner. The augmentation in the trust values show that there is augmentation in the number of paths having high trust values which indicates that the suggested TBVN protocol is more efficient.

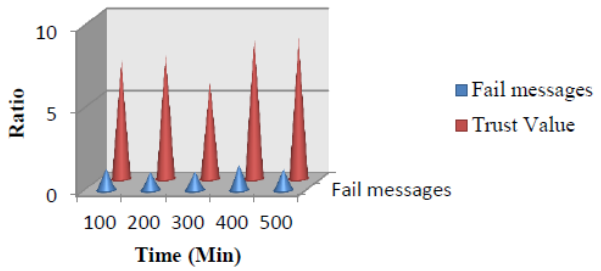

Fig. 5: Rate of Fail Messages and Trust Values for the Data Set 2 Using the Proposed TBVN.

Discussion: The above illustrated figure gives the rate of fail messages and trust values for the suggested TBVN method applied to the data set 2. From the above used clustered cone chart it is clear that trust value attains the optimum value than the fail messages which shows the better presentation of the system. At the value of 400 minutes the node travelled it attains the trust value 10 which shows that it is the 100% trusted path and its fail message rate is very low with the value of 1 which again proves the proposed TBVN effectiveness.

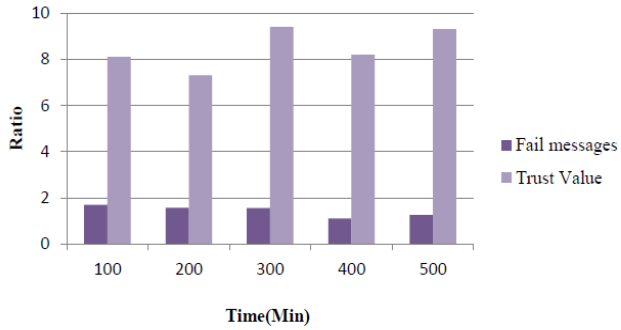

Fig. 6: Rate of Fail Messages and Trust Values for the Data Set 3 Using the Recommended Method.

Discussion: The above illustrated figure gives the rate of fail messages and trust values for the recommended TBVN methodology applied to the data set 3. From the bar chart it is noticed that the fail messages and the trust values varies in the opposite manner. The bar elucidation of the trust values are higher than that of the bar depiction of the fail messages which shows the better efficacy of the suggested TBVN. For example at the 300 minutes the maximum trust value of 9 is attained with less fail messages value of 1.9.

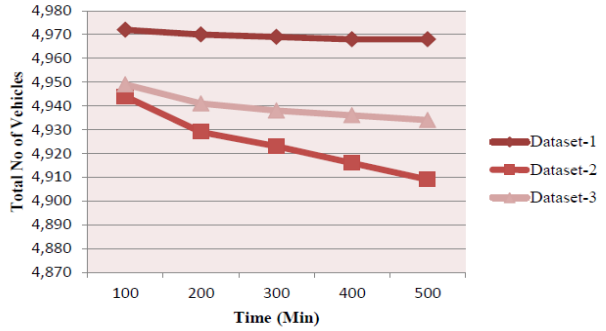

Fig. 7: Variation in Number of Vehicles that are Active Regarding Time.

Discussion: The above illustrated figure gives the overview of number of vehicles that are active amidst the total 5000 vehicles. From the above line with markers chart it is noticed that the pointed curves goes in the downward direction which indicates that as the time augments the number of active vehicles decreases. When the time augments the number of active nodes decreases because as the intention node comes closer only minimum numbers of active nodes are required. For example initially at 100 minutes for data set 1 the number of active vehicles are 4940 and when the time increases and reached 500 minutes the number of active vehicles has been reduced to 4910.

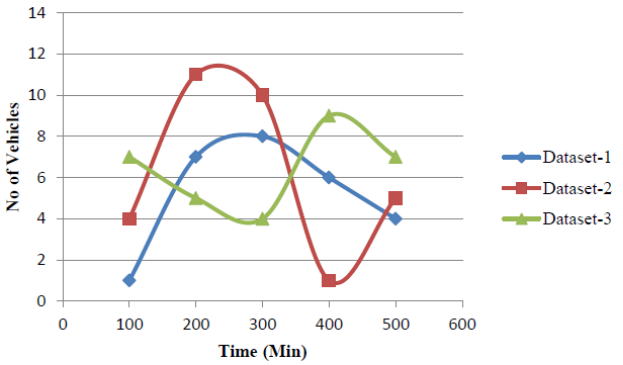

Fig. 8: The Penalty Rate Variation among Vehicles Regarding Time Utilizing the Proposed TBVN.

Discussion: The above illustrated figure gives the penalty rate variation among vehicles regarding time using the proposed TBVN. By observing above scatter chart it is noted that the vehicles that receives the penalty varies in a random manner independent of time. For dataset 2 four vehicles attained the penalty value at the starting 100 minutes travelled. When the time moves by at the 400 minutes only 1 vehicle receives the penalty and then at 500 minutes it receives 5 penalties which shows it is time independent.

4.2. Comparative analysis

4.2.1. Delivery ratio

Packet delivery ratio has been the ratio of the packets number received through the intention to the packet number sent by the sender. It is most salient metric that we must regard as in packet forwarding. It can affect through divergent important component of packet size, group dimension, action range and also nodes mobility. The robust message conduction is signified as the 100% packet delivery. Moreover, 100% delivery signifies receiver get every packets send through sender node prior to time period finishes. The delivery ratio is provided by

$$Delivery\ \ ratio\,(d) = \frac{\text{number of packet received by the destination}(P_R)}{\text{number of packet sent by the sender}(P_S)}$$

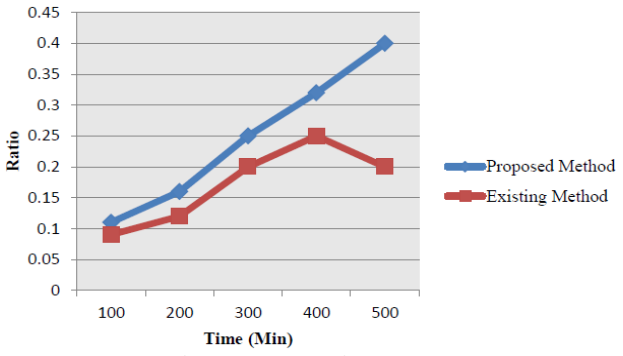

Fig. 9: Comparison of Delivery Ratio of Proposed Method with the Customary Methodology Using the Dataset 1.

Discussion: The above illustrated figure gives the comparison of the proposed TBVN with the customary methodology for another data set. From the graph it is noticed that the curve plotted for the proposed TBVN goes in a rising manner which indicates that delivery ratio of the intended TBVN is high compared to that of the customary methodology. The huger the delivery ratio is, the more vehicles are willing to forward packets. The higher the value of the delivery ratio the possibility of packet loss is minimized which shows the better performance of the intended TBVN protocol.

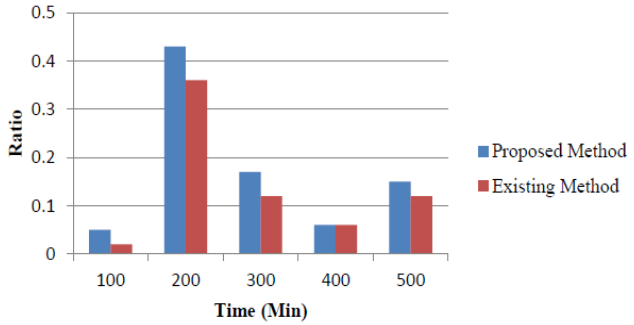

Fig. 10: Comparison of Delivery Ratio of Proposed Method with the Customary Methodology Utilizing the Dataset 2.

Discussion: Comparison of delivery ratio of proposed method with the customary methodology utilizing the dataset 2 is elucidated in the above figure. From the bar chart it is noticed that the bar used for representing the proposed TBVN is higher compared to that of the bar of the prevailing protocol. This indicates that the delivery ratio value attained in second data set using the proposed TBVN is greater than the customary protocol utilizing the same dataset. The delivery ratio varies in a random manner regarding time given.

4.2.2 Computational Cost

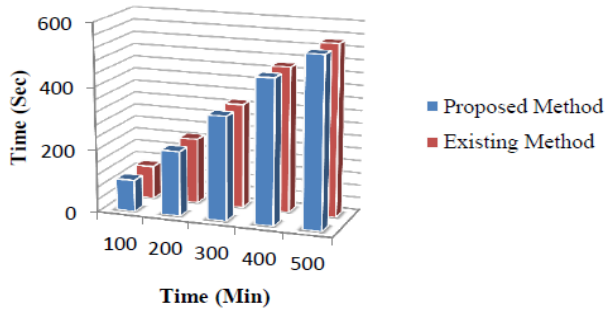

Fig. 11: Comparing Computational Expensiveness of Proposed Method with the Customary Methodology Utilizing the Dataset 1.

Discussion: The figure explains that the computational expensiveness of the proposed TBVN and existing protocol for the used dataset 1. The existing protocol is significantly heavier than our proposed TBVN. The critical reason is that in our proposed TBVN, it selects only the trusted path and transfers the data securely by k-anonymization which avoids the bottle neck at the RSU. On the contrary, the existing protocol adopting Pallier's Cryptosystem as a cornerstone requires one Paillier's encryption on each piece of velocity data, which loads a dramatically increased computational cost on the RSUs which would become a bottleneck when huge numbers of vehicles are passing by especially along the main streets.

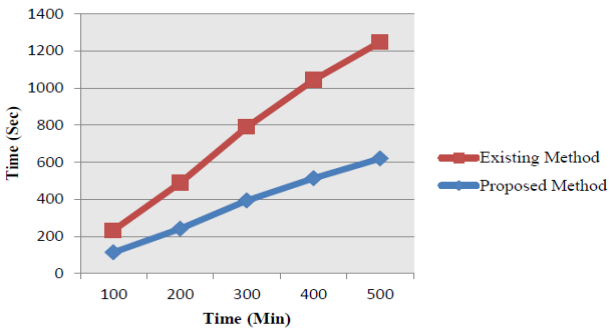

Fig. 12: Comparing Computational Expensiveness of Suggested Methodology with the Customary Methodology Utilizing the Dataset 2.

Discussion: The above elucidated figure gives assay of the suggested TBVN and the existing methodology for data set 2. It is observed that the computational expensiveness of the prevailing method is high matched with that of the suggested TBVN technique. The plotted fields for the computational cost of the recommended TBVN is less matched with that of the existing protocol that presents that our suggested TBVN functions better than the prevailing one.

5. Conclusion

The results were assayed for demonstrating the recommended method's performance with other prevailing methodology. From the assay of the appraisal metric values, we presume that our suggested technique will outperform more improved than any other techniques by having better evaluation metrics. The designing protocol TBVN finds the trusted path of all available nodes for calculating the trust values in every request. Thus the data is shifted in a protected manner. Lastly, the security evaluation and the broad simulations elucidate the efficacy and achievability of our suggested TCBI. In future rather than measuring the trust values we may measure more parameters and also by maximizing it we can prefer the finest path.

References

[1] Whaiduzzaman, Md, Mehdi Sookhak, Abdullah Gani, and RajkumarBuyya, "A survey on vehicular cloud computing", *Journal of Network and Computer Applications*, Vol. 40 pp. 325-344, 2014. https://doi.org/10.1016/j.jnca.2013.08.004.

[2] Hussain Rasheed, and Heekuck Oh, "Cooperation-Aware VANET Clouds: Providing Secure Cloud Services to Vehicular Ad Hoc Networks", *JIPS*, Vol.10, No.1, pp.103-118, 2014.2.

[3] Wang Jin, Yonghui Zhang, Youyuan Wang, and Xiang Gu, "RPRep: A Robust and Privacy-Preserving Reputation Management Scheme for Pseudonym-Enabled VANETs", *International Journal of Distributed Sensor Networks*, 2016.

[4] Taherkhani Nasrin, and Samuel Pierre, "Centralized and Localized Data Congestion Control Strategy for Vehicular Ad Hoc Networks Using a Machine Learning Clustering Algorithm", Vol.17, No.11, 2016.

[5] Louazani Ahmed, Sidi Mohammed Senouci, and Mohammed Abderrahmane Bendaoud, "Clustering-based algorithm for connectivity maintenance in vehicular ad-hoc networks", *In Innovations for Community Services*, pp. 34-38, IEEE, 2014.

[6] Whaiduzzaman, Md, Mehdi Sookhak, Abdullah Gani, and RajkumarBuyya. "A survey on vehicular cloud computing", *Journal of Network and Computer Applications* Vol.40, pp.325-344, 2014 https://doi.org/10.1016/j.jnca.2013.08.004.

[7] Singh Kuldeep, Poonam Saini, Sudesh Rani and Awadhesh Kumar Singh, "Authentication and privacy preserving message transfer scheme for vehicular ad hoc networks (VANETs)", 2015.

[8] Lu Yanrong, Lixiang Li, Haipeng Peng, and Yixian Yang, "Robust ID based mutual authentication and key agreement scheme preserving user anonymity in mobile networks", *KSII Transactions on Internet & Information Systems*,Vol.10, No.3, 2016.

[9] Mandal Monica, Chaitrali Landge, Pramila Gaikwad, Uma Nagaraj, and Ashwini Abhale, "Implementing Storage as a Service in VANET using Cloud Environment", Vol.1, No.5, 2014.

[10] Rajput Ubaidullah, Fizza Abbas, Jian Wang, Hasoo Eun, and Heekuck Oh, "CACPPA: A Cloud-Assisted Conditional Privacy Preserving Authentication Protocol for VANET", *In Cluster, Cloud and Grid Computing (CCGrid)*, pp. 434-442, 2016.

[11] Cho Wonjun, Youngho Park, Chul Sur, and Kyung Hyune Rhee, "An Improved Privacy-Preserving Navigation Protocol in {VANET}s", *JoWUA*, Vol .4, No .4, pp. 80-92, 2013.

[12] Wang, Changji, Dongyuan Shi, XileiXu, and Jian Fang, "An anonymous data access scheme for VANET using pseudonym-based cryptography", *Journal of Ambient Intelligence and Humanized Computing* Vol.7, No.1, pp.63-71, 2016. https://doi.org/10.1007/s12652-015-0301-z.

[13] Jinyuan Sun, Chi Zhang, Yanchao Zhang, and Yuguang Fang, "An Identity-Based Security System for User Privacy in Vehicular Ad Hoc Networks", Vol.21, No.9, 2010.

[14] Chim Tat Wing, Siu-Ming Yiu, Lucas CK Hui, and Victor OK Li, "VSPN: VANET-based secure and privacy-preserving navigation", *IEEE Transactions on Computers*, Vol.63, No.2, pp.510-524, 2014. https://doi.org/10.1109/TC.2012.188.

[15] Kaushik, Sapna S. "Review of different approaches for privacy scheme in VANETs." *Int. J. Adv. Eng. Technol,* Vol. 5, pp.2231-1963 2013.

[16] Lin, Xiaodong, and Xu Li. "Achieving efficient cooperative message authentication in vehicular ad hoc networks." *IEEE Transactions on Vehicular Technology*, Vol .62, No. 7, pp. 3339-3348, 2013. https://doi.org/10.1109/TVT.2013.2257188.

[17] Zhang Jianhong, and Yuwei Xu, "Privacy preserving authentication protocols with efficient verification in VANETs", *International Journal of Communication Systems*, Vol. 27, No.12 pp.3676-3692, 2014. https://doi.org/10.1002/dac.2566.

[18] Wang Yimin, Hong Zhong, Yan Xu, and Jie Cui, "ECPB: Efficient Conditional Privacy-Preserving Authentication Scheme Supporting Batch Verification for VANETs", *International Journal of Network Security*, Vol. 18, No. 2, pp. 374-382, 2016.

[19] Zhou, Jun, 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, 2016. https://doi.org/10.1109/TIFS.2015.2407326.

[20] U. Rajput; F. Abbas; H. Oh, "A Hierarchical Privacy Preserving Pseudonymous Authentication Protocol for VANET," *in IEEE Access*, No.99, pp.1-1, 2016.

[21] S. Biswas and J. Mišić, "A Cross-Layer Approach to Privacy-Preserving Authentication in WAVE-Enabled VANETs," *in IEEE Transactions on Vehicular Technology*, Vol. 62, No.5, pp. 2182-2192, 2013. https://doi.org/10.1109/TVT.2013.2238566.

[22] Sun, Jinyuan, Chi Zhang, Yanchao Zhang, and Yuguang Fang, "An identity-based security system for user privacy in vehicular ad hoc networks", *IEEE Transactions on Parallel and Distributed Systems* Vol. 21, No. 9, pp. 1227-1239, 2010. https://doi.org/10.1109/TPDS.2010.14.

[23] Saxena, Neetesh, Santiago Grijalva, Victor Chukwuka, and Athanasios V. Vasilakos, "Network Security and Privacy Challenges in Smart Vehicle-to-Grid", *IEEE Wireless Communications*, 2017. https://doi.org/10.1109/MWC.2016.1600039WC.

[24] Taha, Sanaa, and XueminShen, "A physical-layer location privacy-preserving scheme for mobile public hotspots in NEMO-based VANETs", IEEE Transactions on Intelligent Transportation Systems, Vol.14, No.4, pp.1665-1680, 2013. https://doi.org/10.1109/TITS.2013.2265311.

[25] Yaqoob Ibrar, Iftikhar Ahmad, Ejaz Ahmed, Abdullah Gani, Muhammad Imran, and Nadra Guizani, "Overcoming the key challenges to establishing vehicular communication: Is sdn the answer?", *IEEE Communications Magazine* Vol. 55, No. 7, pp. 128-134, 2017. https://doi.org/10.1109/MCOM.2017.1601183.