ISSN 2278-3091
Volume 8, No.1.4, 2019
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse2581.42019.pdf
https://doi.org/10.30534/ijatcse/2019/2581.42019

Using Traffic Control Scheme In Intelligent Transportation System

Ali Ghasempour[1], Zurina Mohd.Hanapi[2], Mohammad Salehi[3], Zeinab Vahdati[4]
Faculty of Computer Science and Information Technology, University Putra Malaysia (U.P.M), Malaysia
[1]ali.ghasempor@ieee.org
[2]zurinamh@upm.edu.my
[3]mohammad.salehi@ieee.org
[4]zvahdati70@gmail.com

ABSTRACT

Smart transportation is one of the rapidly developing fields among companies and researchers. Intelligent Transportation Systems (ITS), is a new transportation system which aim to resolve variety of road traffic issues, such as traffic accidents and congestion with cutting-edge technologies. Vehicular Communication Systems (VCS) is main part of ITS's communication which is responsible for key distribution, key management among vehicles and security managers. To speed up key propagation and facilitate the calculation of crossing domain vehicles, there are different algorithms however only some of them consider controlling traffic flow. Traffic congestion has direct effect on key transferring so it is necessary to controlling traffic. In this paper, we proposed traffic control management scheme to characterize, controlling of traffic flow for increasing predictability of crossing domain and increasing safety with adjusting the acceleration of the vehicles. Parametric analysis based on manual calibration model with trial and error technique in mathematics is used to propose traffic control algorithm. At the same time two-way roads and different begin position for each vehicle have been measured. The results show controlled pattern, increasing predictability as well as decreasing key transferring time because of vehicles travel same amount of distance in domain.

Key words: Intelligent Transportation System (ITS), Traffic Control, Key Management, Vehicular Communication

1 INTRODUCTION

Cyber-Physical Systems (CPS) is new terminology in the embedded system area that combined software, hardware, networking, and algorithm to design a model to facilitate human life. There are lots of examples on CPS, like a mobile phone or smart gird. One of the greatest usages of CPS is on transporting industry. Currently, researchers are focusing on providing more safety and convenient travelling using an Intelligent Transportation System (ITS). ITS is using wireless sensors and network protocols on vehicles to communicate and transfer messages securely for providing more safety on roads. According to the U.S Department of Transport, it is possible for prevention 82% of the accident by using intelligent transportation [1]. Vehicle Communication System (VCS) is ledger for transferring messages as well as keys between vehicles. This communication can be Vehicle to Vehicle (V2V) or Vehicle to Infrastructure (V2I).

One of the main components of every transportation system is traffic flow control. Traffic control is not new research area however importance of this field in urban development makes it a favorite research area. While discussing on traffic flow some new terms such as Connected and Automated Vehicles (CAV) needs to be considered. CAVs have effect on both local link level and network level of technology side and human side. [2]. Collection of traffic flow data can be achieved by electronic recording devices along with roads. These devices are capable of collecting speed, class and acceleration of vehicles and transmit to related component for further analysis. Comprehensive and accurate study on gathered data can help to improve road infrastructures and prediction of traffic flow in different time interval. [3]

Different patterns and techniques are discussed in traffic control however in general, traffic flow prediction can be categorized into two main categories, non-parametric or parametric statistical model.[4] For non-parametric, we can name neural network [5] and non-parametric regression [6]. On the other hand for parametric analysis, smoothing techniques [7], auto aggressive linear process [8], historical average algorithm, linear and non-linear average algorithm and lastly time-serious analysis. [9]. Alongside with traffic control, researchers are rapidly developing intelligent traffic system. Like other studies ITS is facing different challenges in both security and communication. According to Figure 1, two main research interests in ITS are communication between nodes and managing traffic control in the domain.
The main issues for ITS is communication between ITS entities. [10] highlighted the challenges for the ITS with respect to the communication issues which are:

- distance factor which discussed to provide a reliable connection between nodes. In a multi-hop network, the protocol is needed to verify all transmitted message correctly as oppose with one hop message.

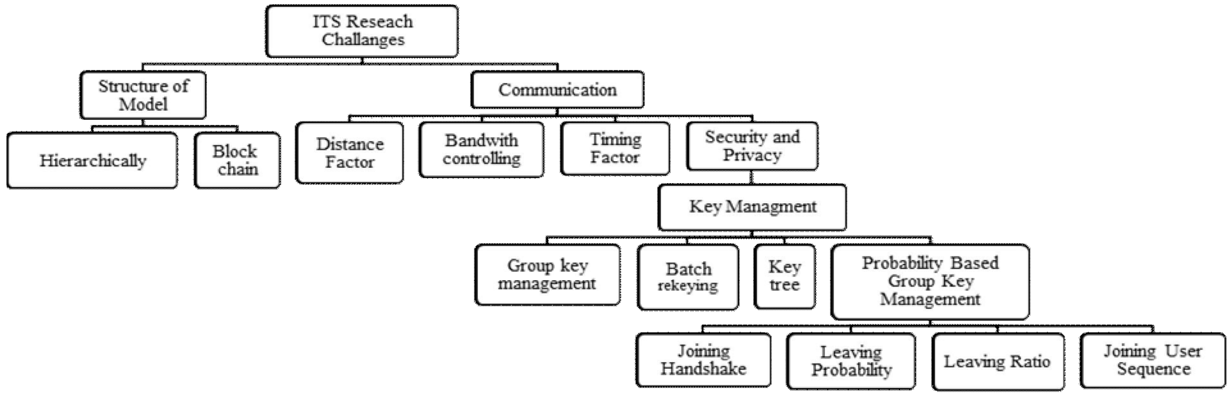

Figure 1: ITS research challenges

- bandwidth and medium access control factor which is about the amount of data transfer from source to other nodes in bit per seconds where data collision to be considered as well.
- time factor is mainly about how often message transfer in a network to avoid any misuse of bandwidth or reducing the performance of nodes. Moreover, time factor has direct relation with traffic flow of roads.
- security and privacy which mostly discussed for providing secure communication and avoiding leaking data on unsecured ledger.

Among mentioned challenges, we focused on time metric especially in intelligence transport. Although some other challenges like security and privacy may look important however scope of this paper is narrowed to improve timing performance compare to current frameworks. To speed up key transferring time and prevent unnecessary key generation different algorithms are suggested. Some of them like leaving probability calculate number of crossing domain nodes based on distribution of time gap between vehicles, thus the system can pass some part key exchanges procedure to another security manager to reduce the time consumed. Other researches such as Mazloumian *et al*. [12] tried to provide optimized simulation platform by macroscopic (fluid-dynamic) simulation approach for traffic flow. They considered probability of leaving domain area however any traffic flow control measurement did not examine.

In this paper, we proposed the traffic control algorithm over intelligence transportation to reduce key transferring time. The algorithm is trying to control and adjust movement of vehicle in domain. Mentioned alteration is done by controlling acceleration of vehicle based on number of nodes in current and other domains. This modification in vehicle acceleration increase vehicle crossing domain's predictability. Therefore, security managers whom are responsible for transferring key among vehicles can transfer keys to vehicles when it is needed. To clarify, generation and transfer keys distribute among security managers to avoid unintended overhead on some security managers. As consequence of this algorithm, road safety increased due to controlled vehicles.

The following sections gives the details of system model and other related traffic control, key generation and simulation methods related to ITS. Section 3, discuss on design of algorithm and implementation. Lastly, section 4, elaborate results of algorithm and compare to other studies.

2. SYSTEM ARCHITECUTE AND RELATED WORKS

Importance of understanding system model cannot be ignored. So far blockchain based and hierarchy system architecture are introduced. In this paper we only consider tree-based model because of most of studies had been done on this framework. In continue, we studied in deep Ao et al. [13] framework to point possible problems in their method. Also Lei et al. [14] adopted same basis of Ao *et al*. framework however blockchain added to architecture. We compare our metrics mostly with Lei *et al*. and with Ao *et al*. researches due to novelty of their work. Both mentioned researches did not consider traffic control in their methods.

2.1 System model

Intelligent transportation system model contains three components, RSU for communicating with vehicles, Security Manager (SM) which is responsible for checking request from RSUs and Central Authority (CA) are connected together to make a connection and key distribution as shown in Figure 2. Moreover, SMs generating keys and communicate to each other to agree on most efficient time to distribute key and certificate in their controlled domain. CA contains base information about vehicles and other related data besides store data in its own database. The hierarchy architecture causes to have single point architecture which is making network vulnerable to potential attack on availability and integrity. In [13], all vehicles accommodate either permanent or temporary certificate to perform joining handshake work. New vehicles must apply the temporary certificate to transfer an Initial Registration Message (IRM) for self-registration at initial participation in ITS environment. Whenever a vehicle changes to another RSU section under the same security area, the permanent certificated will be used. SM and RSUs require collecting vehicle entrance and departure information via BSMs or IRMs to obtain batch rekeying.

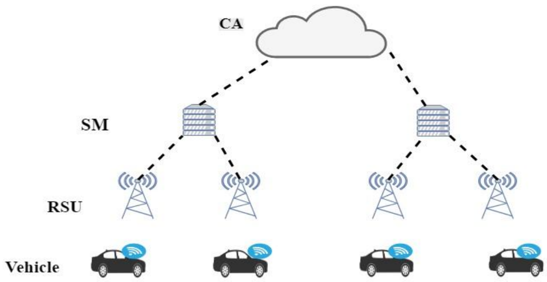

Figure 2 : Traditional ITS structure

The vehicle has communications with another closed by vehicle as well as with infrastructures Roadside Unit (RSU) through On-Board Unit (OBU) via Wi-Fi communication based on the IEEE 802.11p standard. At the same time, WIFI and Bluetooth are considered the most known ledger for communication. Table 1 shows the most useable transmission protocol of ITS. Every vehicle before leaving the factory, a temporary certificate will be assigned to it. Figure 3 shows a basic schema of how vehicle joining to a domain for the first time.

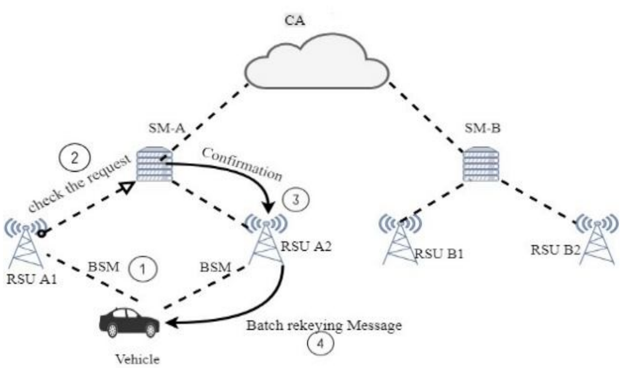

Figure 3 : Change RSU in the same domain

In the first step, it should send the Initial Registration Message (IRM) for self-registration in the ITS environment. The nearest RSU will receive it and check the request and send it to the security manager (SM) and it will be forwarded to the Certificate Authority (CA) that located in the cloud in which all the SMs can have access to it via a safe link. It will check temporary certificate if the vehicle has registered or not and later the CA just send a confirmation message to SM and it will forward it to the RSU. Otherwise, the CA assigned a permanent certificate to the vehicle that can be used for joining handshake and in the next batch rekeying information will be sent to the vehicle [13]. When a vehicle wants to move to another RSU under the same domain, the permanent certificate is useful. As you can see in Figure 4, the vehicle keeps broadcasting the BSM by using previous GK and we assume both previous and new RSU can receive BSMs.

Table 1: Communication technologies in ITS

Wireless Technology	Coverage	Case of Using
WIFI	≈ 50 M	Lots of usage for V2I and V2V
Bluetooth	≈ 10 M	Collect MAC address of phone for OD detection, V2I
2G/3G/4G/5G	Global	Internet, Location, V2V, V2I
WiMAX	≈ 1KM	Internet, Location, V2V, V2I

I

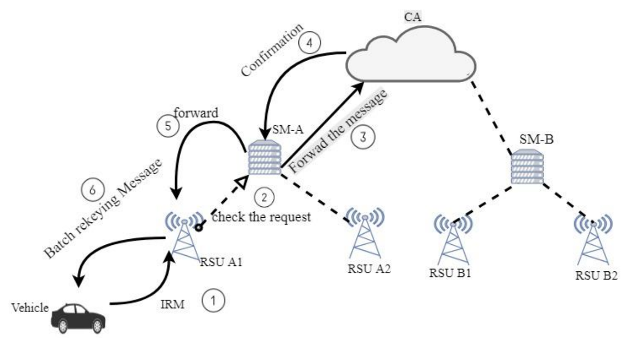

Figure 4 : Joining handshake for a new vehicle

The SM will check the correctness of the request and new RSU gets information about region changing by verified safety beacon message. The new RSU prepares the rekeying message base on confirmation that received and broadcast rekeying occurred in the next batch rekeying interval [13].

Key transferring time is main metric to be measured in this paper. Therefore, understanding key generation and key propagation is necessary for understanding the main idea of this research. Afterwards traffic control researches are discussed to elaborate current ideas related to managing traffic flow.

2.2 Related works

One of most important parts of the ITS is prediction of traffic flow which many research work on this area and predict the traffic flows base on different statistical and machine learning techniques. The neural network is one of common techniques for traffic flow [15] [16].

In [17], they employed deep neural network configuration for traffic prediction. As their main contribution, a new deep learning architecture to predict traffic flows. Their deep learning provides a dramatic enhancement over liner models. In [18], they proposed new way for using Wireless Sensor Network (WSN) which without any direct connection was able to manage the traffic control. The advantage of this model is not required any on board equipment to communicate with WSN that cause to be suitable for undeveloped countries that most of the cars are old. The Traffic lights are controlled by implementing their mode which reduce the overall traffic on the area. They also for enhancement of the system employed V2I communication to provide priority for vehicle like emergency vehicles.

In the wireless network, mobility nodes create the mainstream composition of the network. Batch Rekeying (BR) is a significant way to decrease a huge proportion of rekeying messages rather than Key Tree approaches that try to handle a huge number of nodes. This method assembles all member modification requests within a specific period of time (batch interval) and operates rekeying broadcasting at end of the period (batch edge*)* [19]. In recent years, the heterogeneous vehicular communication network becomes more attractive. They proposed a key management scheme for VCS that combined form, the key transmission and the group batch rekeying scheme between two heterogeneous networks. Leaving probability (LP) is used to decrease rekeying cost in order to gain better efficiency [20].

Leaving the Probability of the mobile node indicates the average number of nodes that leave the group within a rekeying period. In old mobile networks, like LTE and WSN network, joining and leaving act of portable nodes aren't predictable. Therefore, some key management designs require nodes to subscribe to several rekeying periods in order to determine to leave probability. Unfortunately, security vulnerabilities emerge when the system enables users to elect their own subscription period, a malicious user can eavesdrops significant messages by requiring an active period longer than its actual residence time. Different from common wireless mobile networks, probability models are much simpler to perform for vehicle nodes in VCS because they regularly have an expected moving trajectory. For this purpose, a dedicated Leaving Probability calculation algorithm can be improved for VCS scenarios. [14] Calculation of joining or leaving probabilities is based on the distributions of time gaps between vehicles and it has changed over times and it has improved [21].

In other place simulate and predict traffic flow is necessary research to overcome urban transportation issues. Self-driving vehicles are trying to avoid traffic conjunctions and avoid the accident by using wireless sensors network. Also controlling these types of vehicles can improve safety and provide predictable traffic pattern to increase the efficiency of key related transaction. Simulation software proposed by [22] is trying to visualize and simulate vehicles pattern in a road with a different lane.

In previous works, [13] and [14], leaving probability has been used to predict the number of departures that might happen in the RSU domain and send the information of those vehicles to next RSU. The whole proposed of leaving probability is considered the average number of nodes which are leaving the domain within a rekeying interval so current RSU can consider the number of the vehicle will depart from its domain. Thus, the number of keys that should be generated in the next batch rekeying will be declined and the following RSU will take the responsibility of managing those vehicles. Therefore, the following RSU should prepare the key for the new vehicles that are joined and send key in the next batch rekeying interval. However, controlling traffic flow in domain is not discussed in this framework. Based on pervious mentioned studies traffic control leads to improved flow and less congestion on road. Additionally, in intelligent traffic control, it is necessary to avoid unnecessary key generation. Although leaving probability trying to decrease key generation time on security managers however key distribution among nodes need to be considered. Without traffic control this function is not optimized, therefore we come up to design traffic control algorithm over their framework to optimize key transferring time among node.

3. DESIGN

3.1 Overview of algorithm

Our proposed method is optimizing key transfer time in ITS. Somehow this improvement has been done by adding traffic control to pervious researches. As best of our knowledge, [13] and [14] did not consider the number of vehicles that can be derived in the RSU's domain. Moreover, they did not study the capability of the road which may cause conjunction on the road. Therefore, the novel idea is to consider how many vehicles should exist in this domain to have minimal overhead on key distribution.

The traffic congestion is expected to decrees by proposed algorithm to avoid unbalanced number of vehicles in each domain. As an example one domain faces high traffic flow another one works with less than 50% of its capacity. The key point of this model is all vehicles tried to traverse the same distance. Furthermore, in the same period of time, the safety interval considered, based on vehicles speed. Meanwhile, in case of congestion, RSU would decide to decline the speed of vehicles in a domain. RSU is responsible for analyzing domain and make light traffic to avoid the traffic jam. For instance, if it realized that the traffic jam happens in the next domain it will decrease the speed of cars until the problem solved in the following domain.

Proposed algorithm considers the number of nodes which are alive in the domain and calculated by SM. In consequence SM trying to avoid the instability number of incoming and outcoming nodes in the domain. Secondly, the SM manages the acceleration of nodes to get the minimum odd behaviour. Mentioned controlling algorithm has been implemented by manual calibration model to get most satisfied parameters. The calibration model follows trial and error technique in mathematics to analyse the output of model. This analysing trying to achieve least key transferring time between SM and nodes compare to previous studies. Algorithm 1 elaborate manual calibration technique for traffic control algorithm.

Algorithm 1 Pseudocode Traffic Control

```
INPUT: Number of nodes in domain
OUTPUT:Acceleration parameter for each vehicles

procedure analysing number of nodes
RSU_DATA ()
for node in nodes do
if current domain node < next domain node
then
   node acceleration decrease
   if current domain node > next domain node then
     node acceleration increase
   else
     keep current acceleration
   end if
end if
end for
    return result []
end procedure
```

3.2 Platform and performance metrics

A. Platform and tool

For simulating intelligent traffic control environments, we used Python 3.7 as programming language. This implementation had been done on computer with CPU i7-7500, memory 16 GB running on Linux Mint 18. Python had been chosen due to functionality and wide range of libraries for cryptography algorithm which is basic of this study [18].

B. Simulation parameters and performance metrics

Simulation parameters are categorized into two sections. First one for measure number of vehicles are passing a domain. Time (second) and number of vehicles are considered as simulation parameters. In second place to analyse our proposed algorithm, key transferring time between vehicles and security managers as well as traffic level (vehicle/hour/road) considered. Key transferring time is suitable metrics to compare our method with Lei *et al.* method. They measured their key transferring time among components, so we can easily validate our method.

Network topology is based on traffic regulatory in world. According to Australia transport documents [23], the safe following distance is much longer than a car length and it is depending on three factors: vehicle's speed, driving conditions, type of vehicle. The safe distance is usually longer than a car length and at least two second behind the vehicle in front during ideal conditions. Also, it should increase one second for every three meters of trailer length (vehicle towing a trailer or caravan). In the poor condition the distance should be double and if the car is heavy the distance must be increased.

In general, for controlling the speed of the vehicle in the same domain, we hired kinematics physics law about controlling acceleration of each vehicle. The following formula is declaring the travelled distance is physics which is mostly applied all of the cinematic problems:

$$x = \frac{1}{2} \times a \times t^2 + V \times t + V_0 + x_0 \qquad (1)$$

Where x is distance is passed during t time, with acceleration a and starting speed V_0, Also we consider two-way path and may the vehicle is not starting from the beginning of path. So x_0 is considered [24]. Again, we considered our path is a two-way path, therefore, the RSU cannot detect which way the vehicle is going to, and so we need global rules to manage the acceleration. Our algorithm is based on the statistical model that trying to keep the traversed distance of vehicle at the same amount.

C. Dataset

Based on other researchers, simulation method is used for generating standard dataset for analysing performance metrics. We coded and implement other significant studies, then used generated data and input for our algorithm. The dataset verification has been done be achieving same results from other accepted researches.

3.3 Implementation

These assigned acceleration factors are based on the result for 20000 times of running framework. Also as we observed the number of the vehicle in high saturated traffic in Beijing is not passing over 15000 vehicles per hour [14] which shows 20000 times that our framework running is more than number of vehicle passing in one of most crowed road in the world. To implement, we ran the framework for 20000 times. The acceleration factor and number of nodes was changed from time to time to get the best result. Due to the base work which estimated for 2000 transaction, therefore, we step forward to analyze what would be the pattern for a higher number of nodes. Also, we tested the algorithm for 10, 100, 200, 1000 times from beginning to see if there is any miss behavior related to the number of nodes. Fortunately, all of the diagrams follow the same patterns; therefore, we concluded the 20000 times is enough for our analysis. Table 2 shows traffic control algorithm behaviour with manual calibration method.

Table 2: Acceleration factor depends on the number of nodes in the domain base of Traffic Control Algorithm

Number of nodes	Acceleration factor
0 - ¼ *(0% - 25 %)*	*× 1*
1/4 – ¾ *(26 % -75 %)*	*× (- 0.1)*
3/4 – 9/10 *(76 % - 90 %)*	*× abs (current acceleration)*
9/10 – 10/10 *(91 % - 100 %)*	*× (- 0.2)*

The idea behind our method is to avoid any miss behaviour of the vehicle while crossing the domain to make probability of leaving more The Predictable. Proposed model provides a better result in group batch rekeying with considering the capacity of a domain that leads to the best performance in system.

4. DISCUSSION AND RESULTS

We implemented the intelligent transport system framework by simulating same structure for analyzing the result of our algorithm. Figure 5 shows vehicles behaviour in the domain without any traffic control. According to the graph the traversed distance by each vehicle is not same as other vehicles in domain. This pattern causes predication for key passing and key generation time increase. Also predication algorithm efficiency such as leaving probability downgrades

due to this fact that vehicles can travel different distance in time unit. On the other hand, Figure 6 discussing on proposed traffic control which improving predictability of departure and joining a domain. According to result, traversed distance is controlled to help key related procedures such as key transfer and key generation, improve their time consumption. Additionally, probability of leaving prediction is more precisely because of most of vehicles traverse same amount of distance in time unit. Although some of the vehicles have odd behaviour, in overall result is promising.

After all, to prove our model is increasing efficiency in key related materials, we compare transfer key time in our proposed model to Lei *et al.* (Lei, Cruickshank, Cao, et al., 2017). According to Figure 7, key transferring time in proposed model need less time in comparing to Lei *et al.* model in heavy traffic. Besides we analysed skewness of our algorithm in large traffic. Based on Figure 8, still our method delivers key in efficient time compare to other studies.

All in all, traffic control method is focusing on time parameter in intelligent transport system field. Key transferring time dramatically decreased. By our perception controlling the traffic flow can increase safety of roads and avoiding heavy jam in populated cities.

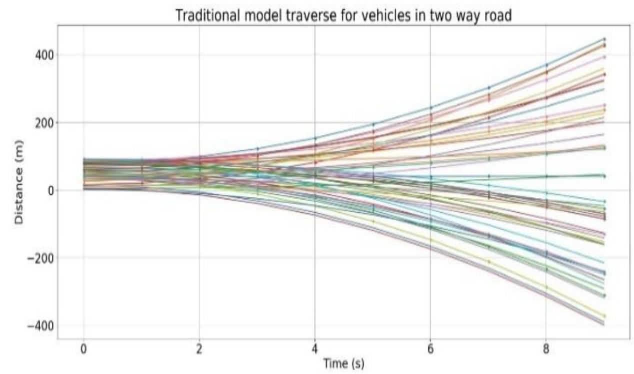

Figure 5: Unmanaged traffic control for 50 nodes based on base work. Each node traveled a different amount. The mines travel means the opposite way in the two-way path

Figure 6: After applying traffic control algorithm, most of nodes travel same distance using proposed framework therefore the prediction will be improving

5. CONCLUSION

In this paper, we discussed issues of Intelligent Transportation System (ITS) and proposed the method to control traffic flow to increase predictability and efficiency of cryptographic parties. Traffic control algorithm with manual calibration technique is used to achieve optimized parameter for vehicles acceleration. Moreover, the time consummation for whole of the system is decreasing because of avoiding unnecessary key transferring. Additionally, passenger’s safety raises by framework is improving collaboration between other vehicles in domain for providing most accurate acceleration based on traffic flow. Traffic control can easily apply to real life while nowadays self-driving vehicle is becoming much more popular. Last but not least, this framework may apply to other vehicular cases because of improving predictability of nodes.

ACKNOWLEDGEMENT

This work was supported by Putra Berimpak research grant UPM/800-3/3/1/GPB/2018/9659400.

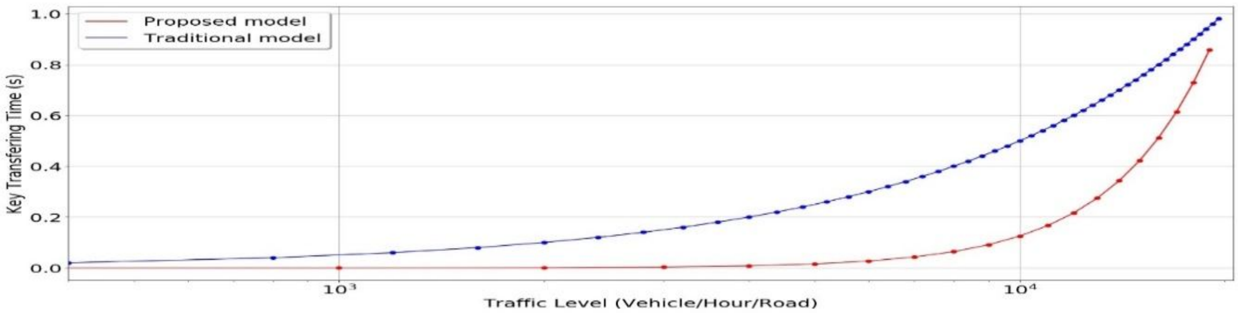

Figure 7. Comparing key transferring time of proposed model with Lei et al. model

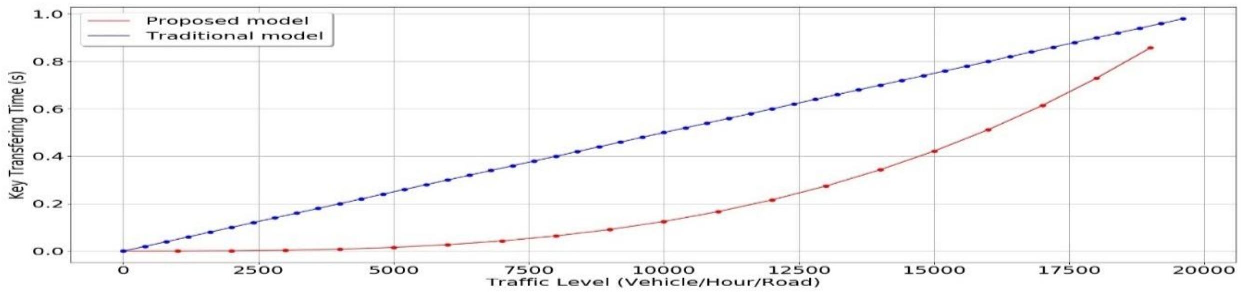

Figure 8. Skewness of proposed model in high traffic level in compare to Lei et al. model

REFERENCES

1. J. B. Kenney, **Dedicated Short-Range Communications (DSRC) Standards in the United States,** *Proc. IEEE*, vol. 99, no. 7, pp. 1162–1182, Jul. 2011. https://doi.org/10.1109/JPROC.2011.2132790
2. S. Calvert *et al.*, **Traffic Flow of Connected and Automated Vehicles: Challenges and Opportunities,** Springer, Cham, 2018, pp. 235–245. https://doi.org/10.1007/978-3-319-60934-8_19
3. M. Jiber, I. Lamouik, Y. Ali, and M. A. Sabri, **Traffic flow prediction using neural network**, in *2018 International Conference on Intelligent Systems and Computer Vision (ISCV)*, 2018, pp. 1–4. https://doi.org/10.1109/ISACV.2018.8354066
4. B. Ghosh, B. Basu, and M. O'mahony, **A Bayesian Time-Series Model For Short-Term Traffic Flow Forecasting,** *J. Transp. Eng.* , vol. 133, no. 3, pp. 180–189, 2007. https://doi.org/10.1061/(ASCE)0733-947X(2007)133:3(180)
5. V. P., **Alternative Approaches To Short Term Traffic Forecasting For Use In Driver Information Systems,** *Transp. traffic theory*, vol. 12, pp. 485–506, 1993.
6. G. A. Davis and N. L. Nihan, **Nonparametric Regression and Short□Term Freeway Traffic Forecasting**, *J. Transp. Eng.*, vol. 117, no. 2, pp. 178–188, Mar. 1991. https://doi.org/10.1061/(ASCE)0733-947X(1991)117:2(178)
7. M. E. Bell and M. J. Demetsky, **Macroeconomic analysis of the linkages between transportation** `````````**investments and economic performance,** no. 1453. Transportation Research Board, National Research Council, 1997.
8. H. R. Kirby, S. M. Watson, and M. S. Dougherty, **Should we use neural networks or statistical models for short-term motorway traffic forecasting?**, *Int. J. Forecast.*, vol. 13, no. 1, pp. 43–50, Mar. 1997. https://doi.org/10.1016/S0169-2070(96)00699-1
9. S. V. Kumar and L. Vanajakshi, **Short-term traffic flow prediction using seasonal ARIMA model with limited input data**, *Eur. Transp. Res. Rev.*, vol. 7, no. 3, p. 21, Sep. 2015. https://doi.org/10.1007/s12544-015-0170-8
10. A. Maimaris and G. Papageorgiou, **A review of Intelligent Transportation Systems from a communications technology perspective**, in *2016 IEEE 19th International Conference on Intelligent Transportation Systems (ITSC)*, 2016, pp. 54–59. https://doi.org/10.1109/ITSC.2016.7795531
11. M. Rudack, M. Meincke, and M. Lott, **On the Dynamics of Ad Hoc Networks for Inter Vehicle Communications (IVC)**, *Univ. Hann.*, 2002.
12. A. Mazloumian, N. Geroliminis, and D. Helbing, **The spatial variability of vehicle densities as determinant of urban network capacity**, *Philos. Trans. R. Soc. A Math. Phys. Eng. Sci.*, vol. 368, no. 1928, pp. 4627–4647, Oct. 2010. https://doi.org/10.1098/rsta.2010.0099
13. L. Ao, C. Ogah, P. Asuquo, H. Cruickshank, and S. Zhili, **A Secure Key Management Scheme for Heterogeneous A Secure Key Management Scheme for Heterogeneous Secure Vehicular**

Communication Systems Secure Vehicular Communication Systems, *ZTE Commun.*, vol. 21, no. 3, p. 1, 2016.

14. A. Lei, H. Cruickshank, Y. Cao, P. Asuquo, C. P. A. Ogah, and Z. Sun, **Blockchain-Based Dynamic Key Management for Heterogeneous Intelligent Transportation Systems,** *IEEE Internet Things J.*, vol. 4, no. 6, pp. 1832–1843, Dec. 2017. https://doi.org/10.1109/JIOT.2017.2740569
15. W. Zheng, D.-H. Lee, and Q. Shi, **Short-Term Freeway Traffic Flow Prediction: Bayesian Combined Neural Network Approach**, *J. Transp. Eng.*, vol. 132, no. 2, pp. 114–121, Feb. 2006. https://doi.org/10.1061/(ASCE)0733-947X(2006)132:2(114)
16. R. Li and H. Lu, **Combined Neural Network Approach for Short-Term Urban Freeway Traffic Flow Prediction**, *Lect. Notes Comput. Sci.*, vol. 5553, pp. 1017–1025, 2009. https://doi.org/10.1007/978-3-642-01513-7_112
17. N. G. Polson and V. O. Sokolov, **Deep Learning For Short-Term Traffic Flow Prediction,** *Transp. Res. Part C Emerg. Technol.*, vol. 79, pp. 1–17, Jun. 2017. https://doi.org/10.1016/j.trc.2017.02.024
18. W. U. Rahman, M. Ashraf, and A. Iqbal, **Intelligent Traffic Control System for Wireless Sensor Networks and GSM Without Direct Communication With on Road Vehicles**, *GSJ*, vol. 7, no. 1, 2019.
19. X. S. Li, Y. R. Yang, M. G. Gouda, and S. S. Lam, **Batch rekeying for secure group communications**, in *Proceedings of the tenth international conference on World Wide Web - WWW '01*, 2001, pp. 525–534.
20. O. Zakaria, A.-H. A. Hashim, and W. H. Hassan, **An Efficient Scalable Batch-Rekeying Scheme For Secure Multicast Communication Using Multiple Logical Key Trees**, *IJCSNS Int. J. Comput. Sci. Netw. Secur.*, vol. 14, no. 11, 2014.
21. M. Rudack, M. Meincke, and M. Lott, **On the Dynamics of Ad Hoc Networks for Inter Vehicle Communications (IVC).** 2002.
22. P. Gora and I. Rüb, **Traffic Models for Self-driving Connected Cars**, *Transp. Res. Procedia*, vol. 14, pp. 2207–2216, Jan. 2016. https://doi.org/10.1016/j.trpro.2016.05.236
23. Queensland Goverment, **Safe following distances**, 2015. [Online]. Available: https://www.qld.gov.au/transport/safety/rules/road/distances.
24. J. W. David Halliday, Robert Resnick, **Fundamental of Physics**. Wiley, 2010.