Calibration of Car-Following Behavior to analyze malicious vehicles

Lalit Gawande Pragati Patil

W.C.C. Abha Gaikwad-Patil College of Engineering, NagpurINDIA

ABSTRACT

The Research calibration process is a basic condition of traffic model which uses car following behaviors for road traffic studies. The transmission channel between moving vehicles in real time traffic environment is modeled in road traffic and neighboring environment adjacent to the road. The choice of input parameters, which are used in the calibration process, influences the success of the calibration process itself; therefore, the goal is to choose parameters with a larger influence on the modeling process. First, it takes velocity, velocity difference and position difference observed in last few time intervals as input. The second car following model is built in a data-driven way in which we reduce human interference to the minimum degree. The e-Road project is an attempt to achieve the aforementioned goals by providing scalability. The decision to rebroadcast the message is also affected by the situation of the receiver, such as the distance to the original sender, speed, traffic density, and the interest table of neighboring vehicles i.e. history table. The experimental basis was a one-lane roundabout, and the tool used for traffic simulation was the traffic model. This paper describes a detailed analysis of car-following input parameters and its influence on the modeled traveling time. All these findings provide a novel study of traffic flow theory and traffic simulation and used to detect intelligent traffic system. It detects the malicious behavior of various vehicles. The algorithm was implemented in C# dot net and tested under Windows system.

Keywords:Car-following input parameters, input parameters for the process of calibration.

I.INTRODUCTION

In order to increase the probability of verifying potential malicious vehicles position, we keep track of vehicle movements. By exchanging packets in a cell, each vehicle knows the exact position of all other remaining vehicles in a cell. Vehicles in a cell can query the position of a specified vehicle among the neighbors in the cell. When receiving responses from neighbors and computing these positions, the requester comes to an agreement about all the neighbors' position [1]. With local tower detected data, oncoming traffic's radar detected data, and trusted neighbors' data in hand; we apply cosine similarity to these data. If the cosine similarity score is above a threshold value, we will accept the data, otherwise, it is dropped. With the accepted data, we build a history of vehicle movements, or a History table [3]. The basic idea is that a vehicle without position history is not trustable, just like a person without credit history can't obtain a loan. The decision to rebroadcast the message is also affected by the situation of the receiver, such as the distance to the original sender, speed, traffic density, and the interest table of neighboring vehicles. When the position of receiving vehicle is announced, the observer checks the History table to verify the position based on movement consistency [2]. If there is any inconsistency, the particular record is more than likely to be picked up for verification. By comparing what is heard and seen, a vehicle can determine out the real position of the neighbors and isolate. Due to the limitation of tower visibility range, we need to combine local security to achieve global security[5]. We present preset position-based cells to create a communication network by securely exchanging packets among cells. Besides, we propose a method to challenge and confirm the position of a vehicle in a remote cell.

II.LITERATURE SURVEY

For Detection System in an automotive context, several publications propose anomaly detection based on clearly defined and specified normal onboard system behavior and suggest specification-based attack detection [5], assuming that a representation of the normal behavior of communication and ECUs can be derived from the system[8]. Policy and the expected usage of a component, which is then compared to the observed behavior. In a set of in-vehicle detection sensors is described from an abstract point of view [9]. Details on implementation and verification are not given in the above publications. On the commercial side, Towers provides runs on a CAN bus accessible ECU, telemetric controller or infotainment unit, and continuously monitors the events in order to identify new threats. According to in the in-vehicle network and blocks them in real time [11]. To the best knowledge of the authors of this paper, details about the approaches used in the Towers and Argus products are not publicly available. In general, systems usually do not have knowledge of the vehicle applications, thus lacking the connection between the reported security problems and the affected critical behavior. The systems can be based on several different technologies; however, the system is only verified on synthetic data. Such systems often deliver a very low false positive rate, but they usually identify outliers based on inspection of single events [10]. Thus, they might miss attacks based on valid events sent in the wrong context. Predictive security analysis for event-driven processes has been introduced. Here, we use a similar approach but a different realization adapted for the requirements of the automotive domain.

III. PROPOSED WORK

A vehicle can collaborate with the real position of neighbor's vehicle and detect malicious vehicles, thus it achieved local security. Due to this inherent limitation of radar spatial penetration, we cannot directly use this process to achieve global security but can be used local security as a basis for achieving global security. Although we are using preset position-based cells through which we can achieve local security to create a local communication network among all the neighboring vehicles. Global security is achieved by exchanging packets among cell members and verifying neighboring vehicles' positions using oncoming traffic. Each vehicle generates information about the state of the traffic based on both what is seen and what is received from other vehicles in the system. In this project, we propose a new solution to secure the position information. The goal of our work is to provide a secure topology for a VANET and to build a secure network for applications. The basic idea is the famous saying: "seeing is believing". We use radar as a virtual "eye" of a vehicle. Although the "eyesight" is limited due to the limitation of radar transmission range, a vehicle can "see" surrounding vehicles and hear reports.

IV. FIGURES AND TABLES

In this project, we are using a highway-based scenario, and the cells are having 100 meters in radius, therefore, we select 20-30 meter overlaps as interval captured by monitoring devices. When vehicles are close to the interval of two cells in the same route, then that may be chosen as following vehicles. The need of routers depends on the transmission range between all neighboring vehicles. If the transmission range can reach the next cell leader without needing an intermediate hop, then there is no need to have cell routers.

The steps to form a network cell are:

- By consulting loaded digit map, each vehicle can decide the width of the overlap regions between two cells.
- Partition the digital map into cells, for example, 100 meter-radius cells, making sure the overlaps; vehicles decide its cells based on its position coordinates and preset digital maps.

When a new vehicle enters the system, it waits for 200ms during which it hears the information transmitted by other members of the cell and learns the cell leader's ID. The new vehicle also activates its tower to detect its neighbors. At the end of the time slice, it sends its position information as well as position information of its neighbors. If it was not able to detect the cell leader, it sends a query asking the address (ID) of the cell leader. If no response comes, then new vehicle takes over as a cell leader and announces its new role. In order to increase the probability of verifying potential malicious vehicles position, we keep track of vehicle movements. By exchanging packets in a cell, each vehicle knows the exact position of all other remaining vehicles in a cell. Vehicles in a cell can query the position of a specified vehicle among the neighbors in the cell. When receiving responses from neighbors and computing these positions, the requester comes to an agreement about all the neighbors' position[1]. With local tower detected data, oncoming traffic's radar detected data, and trusted neighbors' data in hand; we apply cosine similarity to these data. If the cosine similarity score is above a threshold value, we will accept the data, otherwise, it is dropped. With the accepted data, we build a history of vehicle movements, or a History table[3]. The basic idea is that a vehicle without position history is not trustable, just like a person without a credit history cannot obtain a loan. When it received a position of vehicle it announced it and the observer check the History table to verify their position based on movement consistency. If there is any inconsistency, the particular record is more than likely to be picked up for verification. A verification request can be sent in two different ways. First, using the vehicles in the same direction and secondly, making the opposite direction vehicles verify the vehicle. The request message travel till it reaches the vehicle which is in direct line of sight of the disputed vehicle. A response message is then sent back to the requester. A positive response would validate the record. The request and response message need not wait for next transmission to happen. They are transmitted as soon as they are received. Because of this, the vehicle might receive two confirmations: one from reverse direction vehicles and another from same direction vehicle. Since there is less incentive for reverse direction vehicles to lie, reverse direction confirmation is given more weight.

We extended a microscopic traffic simulator based on the microscopic transport simulator, which features a realistic traffic model. Vehicles in our simulator can accelerate if there is reasonable space ahead, decelerate if the space in front is small or forward vehicles suddenly decelerate, completely stop if there is no way to move or change lane or steadily drive and change lanes. In this project, we use a two-direction highway scenario with two lanes in each direction. The comparison of our algorithm with flooding. In flooding each vehicle within transmission range receives the message and broadcasts it to its neighbors' till it reaches the destination vehicle. Our algorithm needs less number of hops compared to flooding. The next experiment was run to calculate the time taken to detect the malicious vehicles in the system.Aggregation Algorithm: This algorithm performs on the records in the validated dataset in order to place more information in the outgoing broadcast messages. This module might as well update the dataset by replacing the original records with the new aggregate version. This sends module the contents of the records in the validated dataset in a broadcast message.Ratio-based Algorithm: The algorithm divides the road in front of the vehicle to a number of regions. For each region, an aggregation ratio is assigned. The aggregation ratio is defined as the inverse of the number of individual records that would be aggregated in a single record. Each region is assigned to a portion where all the remaining free space in the broadcast message. The aggregation ratios and region portion values are assigned according to the importance of the regions and how accurate the broadcast information about the vehicles in that regionis needed to be. For example, assigning decreasing values to the aggregation ratios and equal values to portion parameters will result in broadcasting less accurate information about regions that are farther away from the current vehicle, since for those regions,each individual record will represent a large number of aggregated vehicles records.

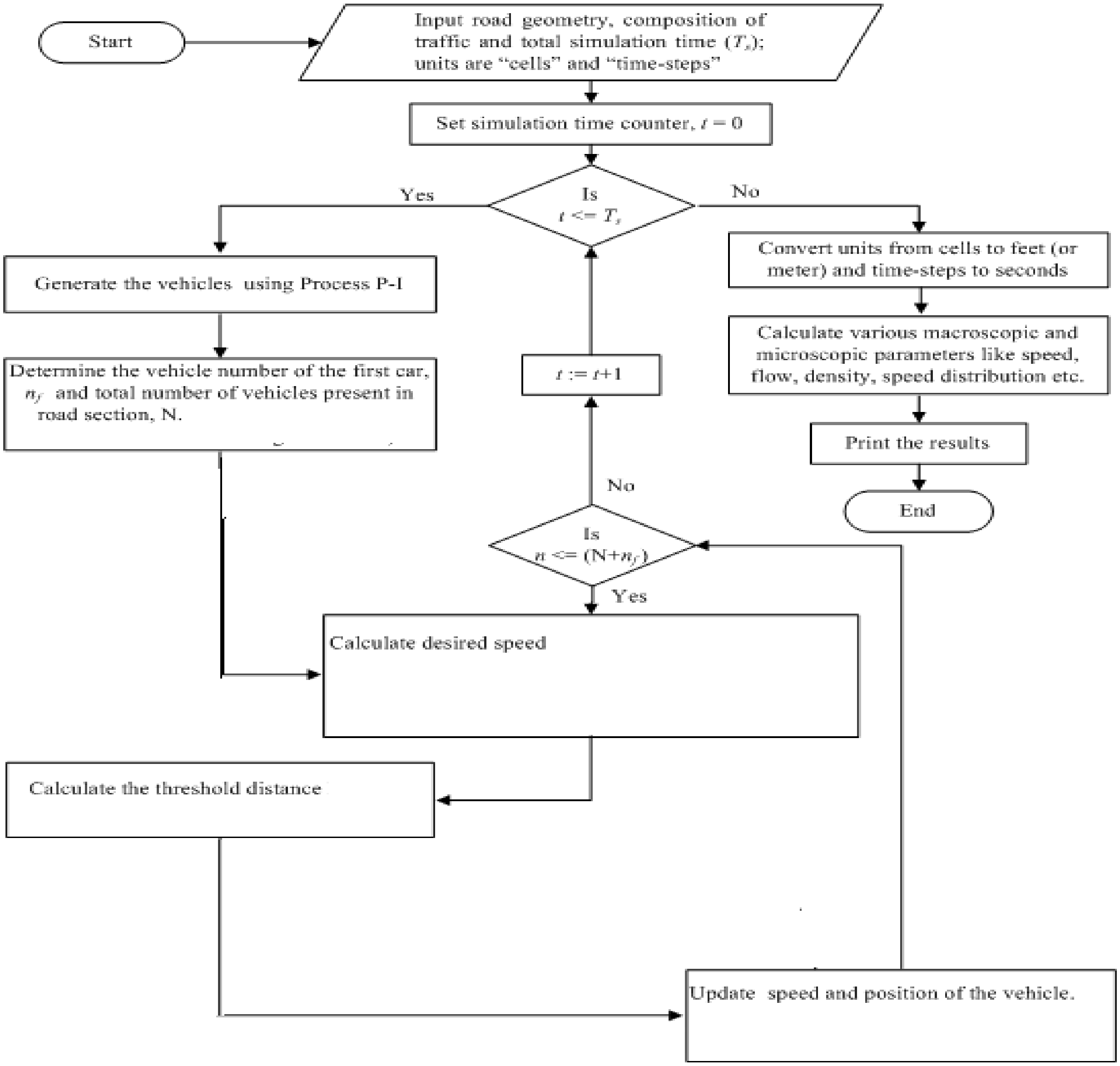
Start
Input road geometry, composition of traffic and total simulation time (T_s); units are "cells" and "time-steps"
Set simulation time counter, $t = 0$
Yes
Is $t <= T_s$
No
Convert units from cells to feet (or meter) and time-steps to seconds
Calculate various macroscopic and microscopic parameters like speed, flow, density, speed distribution etc.
Print the results
End
Generate the vehicles using Process P-I
Determine the vehicle number of the first car, n_f and total number of vehicles present in road section, N.
$t := t+1$
No
Is $n <= (N+n_f)$
Yes
Calculate desired speed
Calculate the threshold distance
Update speed and position of the vehicle.

Figure. 1. Flow chart of traffic flow simulation model

V.CONCLUSION

By comparing what is heard and seen, a vehicle can determine out the real position of the neighbors' and isolate. Due to the limitation of tower visibility range, we need to combine local security to achieve global security. We present preset position-based cells to create a communication network by securely exchanging packets among cells. Besides, we propose a method to challenge and confirm the position of a vehicle in a remote cell. In this project, we propose a new solution to secure the position information. The goal of our work is to provide a secure topology for a VANET and to build a secure network for applications. The basic idea is the famous saying: “seeing believes”. We use radar as a virtual “eye” of a vehicle. Although the “eyesight” is limited due to the limitation of radar transmission range, a vehicle can “see” surrounding vehicles and hear reports. We are using flooding in which each vehicle within transmission range receives the message and broadcasts it to its neighbor’s till it reaches the destination vehicle. Our algorithm needs less number of hops compared to flooding. The next experiment was run to calculate the time taken to detect the malicious vehicles in the system. Detection of false position information and reducing the chances of attack is the key to the success of VANETs. This project focuses on this prime area of traffic. Radar acts as the eye of the system and allows a vehicle to trust the information received from the vehicles within its range.

REFERENCES

[1] Asaithambi, Gowri, and SehleBasheer. "Analysis and modeling of vehicle following behavior in mixed traffic conditions." *Transportation research procedia* 25 (2017): 5094-5103.

[2] Talebpour, Alireza, Hani S. Mahmassani, and Samer H. Hamdar. "Effect of information availability on stability of traffic flow: Percolation theory approach." *Transportation Research Part B: Methodological* (2017).

[3] Zhu, F., &Ukkusuri, S. V. (2017). An Optimal Estimation Approach for the Calibration of the Car-Following Behavior of Connected Vehicles in a Mixed Traffic Environment. *IEEE Transactions on Intelligent Transportation Systems*, *18*(2), 282-291.

[4] Deng, H., & Zhang, H. (2012). Driver anticipation in car following. *Transportation Research Record: Journal of the Transportation Research Board*, (2316), 31-37.

[5] Monteil, J., Billot, R., Rey, D., & El Faouzi, N. E. (2012). Distributed and centralized approaches for cooperative road traffic dynamics. *Procedia-Social and Behavioral Sciences*, *48*, 3198-3208.

[6] Yeo, H., &Skabardonis, A. (2009). Understanding stop-and-go traffic in view of asymmetric traffic theory. In *Transportation and Traffic Theory 2009: Golden Jubilee* (pp. 99-115). Springer US.

[7] Ammari, H.M., Das, S.K., 2008. Integrated Coverage and Connectivity in Wireless Sensor Networks: A Two-Dimensional Percolation Problem. Computers, IEEE Transactions on 57(10), 1423-1434.

[8] Broadbent, S.R., Hammersley, J.M., 1957. Percolation processes. Mathematical Proceedings of the Cambridge Philosophical Society 53(03), 629-641.

[9] Meester, R., Roy, R., 1996. Continuum Percolation. Cambridge University Press.

[10] Almiron, M.G., Goussevskaia, O., Loureiro, A.A.F., Rolim, J., 2013. Connectivity in obstructed wireless networks: from geometry to percolation, Proceedings of the fourteenth ACM international symposium on Mobile ad hoc networking and computing. ACM, Bangalore, India, pp. 157- 166.

[11] Khanjary, M., Sabaei, M., Reza Meybodi, M., 2015. Critical density for coverage and connectivity in two-dimensional fixed-orientation directional sensor networks using continuum percolation. Journal of Network and Computer Applications 57, 169-181.

[12] Treiber, M., Kesting, A., 2013. Traffic Flow Dynamics: Data, Models and Simulation. Springer.

[13] Treiber, M., &Kesting, A. (2013). Microscopic calibration and validation of car-following models–a systematic approach. *Procedia-Social and Behavioral Sciences*, *80*, 922-939.

[14] Wilson, R.E., Ward, J.A., 2010. Car-following models: fifty years of linear stability analysis – a mathematical perspective. Transportation Planning and Technology 34(1), 3-18.

[15] Chakroborty, P., Kikuchi, S., 1999. Evaluation of the General Motors Based Car-Following Models and a Proposed Fuzzy Inference Model. Transportation Research Part C 7 (4), 209–235.

[16] Chakroborty, P., & Kikuchi, S. (2003). Calibrating the membership functions of the fuzzy inference system: instantiated by car-following data. *Transportation Research Part C: Emerging Technologies*, *11*(2), 91-119.

[17] Ciuffo, B., Punzo, V., &Montanino, M. (2012). Thirty Years of Gipps' Car-Following Model: Applications, Developments, and New Features. *Transportation Research Record: Journal of the Transportation Research Board*, (2315), 89-99.

[18] Gipps, P. G. (1981). A behavioural car-following model for computer simulation. *Transportation Research Part B: Methodological*, *15*(2), 105-111.

[19] Ye, F., Zhang, Y., 2009. Vehicle- Type Specific Headway Analysis using Freeway Traffic Data. Transportation Research Record 2124, TRB, Washington, D. C., USA, 222–230.

[20] Brackstone, M., McDonald, M., 1999. Car-following: a Historical Review. Transportation Research Part F 2 (4), 181-196.

[21] Cho, H. J., Wu, Y. T., (2004). Modelling and Simulation of Motorcycle Traffic Flow. IEEE International Conference on Systems, Man and Cybernetics, 7, 6262- 6267.

[22] Lan, L. W., Chang, C.W., 2004. Motorcycle-following Models of General Motors (GM) and Adaptive Neuro-fuzzy Inference System (in Chinese), Transportation Planning Journal 33(3), 511-536.