INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

www.ijprems.com
editor@ijprems.com

Vol. 03, Issue 05, May 2023, pp : 1093-1098

e-ISSN : 2583-1062

Impact Factor : 5.725

IMPACT EVALUATION OF CYBER-ATTACKS ON TRAFFICFLOW OF CONNECTED AND AUTOMATED VEHICLES

V. N. S. Manaswini[1], V. Manisha[2], A. Harani[3], K. Sneha[4], Yeswanth[5]

[1]Assistant Professor, Computer Science Department, Siddhartha Institute of Technology and Science, Hyderabad, Telangana, India

[2,3,4,5]Students, Computer Science Department, Siddhartha Institute of Technology and Science, Hyderabad, Telangana, India

ABSTRACT

Connected and automated vehicles (CAVs) can improve transportation safety and efficiency based on vehicle-to-vehicle (V2V) or vehicle-to-infrastructure (V2I) communications. However, there are potential cyber threats to the communication systems via on-board unit equipped in CAVs and road-side unit. Based on existing traffic flow models, we design an evaluation framework for cyber-attacks on CAVs, and further investigate the impact of proportion of cyber-attacked vehicles, cyber-attack severity, cyber-attack range and traffic demand. Moreover, performance of the transportation system is analyzed based on four indicators, including efficiency, safety, emissions and fuel consumption. The numerical simulation results show that with the increase of cyber-attacked vehicles and higher cyber-attack severity, the negative impact on traffic flow gradually becomes notable with lower capacity, higher risk of rear-end collision, more air pollutants and fuel consumption. In addition,it may lead to accidents and inefficient traffic operations if cyber-attacks occur on position rather than speed, and thus the position-attacked traffic system consumes more energy and emits more pollutants. The findings of this study provide useful information for the prediction of future cyber-attacked traffic, comprehensive evaluation of transportation systems, as well as management of automated highway systems from the perspective of network security.

Keywords: Cyber-attack, Cooperative adaptive cruise control, Connected and automated vehicles, Safety level.

1. INTRODUCTION

In recent years, connected and automated vehicles (CAVs) hasbeen one of prospective applications within the field of intelligent transportation systems (ITS) in the future [1-3]. To predict potential emergencies about CAVs, simulation experiments designed for different traffic scenarios are a fundamental step before launching mature products into the market. To date, many car-following models have been proposed to describe characteristics of traffic flow from microscopic perspective [4-8]. The adaptive cruise control (ACC) system is one of the most popular applications designedfor the control of longitudinal behaviors [9-12]. In addition, asan enhanced version of ACC, the cooperative adaptive cruise control (CACC) system can notably smooth Hazardous traffic flow and improve traffic efficiency [4, 11, 13-19]. Li et al. developed an infrastructure-to-vehicle integrated system that incorporated both ACC and variable speed limit (VSL) to reduce rear-end collision risks on freeways [20]. Shladover et al. analyzed the advantages of CACC based on vehicle-to- vehicle (V2V) communication, including higher accuracy, faster response, and shorter gaps, resulting in enhanced traffic flow stability and possibly improved safety [17, 18, 21, 22]. Infield test, several projects have been conducted for the system designs as well as empirical data analysis [18, 21, 23]. For example, the California Program on Advanced Technology forthe Highway (PATH) attempted to design longitudinalcontrollers, providing an ideal basis for the following studies [11, 13, 14, 21, 24-28].

3 5, May 2023 May

However, advanced technologies always bring both opportunities and challenges. In the transportation field, the opportunities mean improvement of travel efficiency and traffic safety, while the challenges represent risk of cyber-attack, cost increase and moral issues when crashes happen [29-33]. In this paper, we focus on the cyber-attack via communications between on-board units and road-side units. In the previous theoretical researches, simulations have been extensively conducted to demonstrate the safety and stability of the cyber-attacked system [3, 12, 14, 31-41]. Particularly, Li et al. evaluated the influence of slight cyber-attacks on longitudinal safety of CAVs based on nine-vehicle experiments [14]. Wang et al. proposed an extended car-following model and analyzed the linear and nonlinear stability of the traffic flow under cyber-attack [40]. Amoozadeh et al. demonstrated that insider cyber-attacks could cause significant instability of CACC vehicle stream based on simulation, and then put forward several countermeasures [34]. In the aforementioned works, CACC is chosen as the only longitudinally automation control system for CAV simulations. Besides, Petit and Shladover did the first investigation of the potential cyber- attacks specific to automated vehicles with their special needs and vulnerabilities [3]. Jia et al. systematically conducted a survey on platoon-based vehicular cyber-physical systems [42]. Reilly et al. presented a controllability analysis of freeways with coordinated metering to evaluate impact of control system cyber-physical attacks [43]. Generally, much attention has been paid to the communication system and safety analysis, and thus the inherent characteristics of cyber-attack need furtherexplorations. Also, more investigations should be conducted onits impact on traffic flow stability, efficiency, emissions and fuel consumption.

In this paper, we differentiate from the previous studies andemphatically address the following questions:

(1) What factors influence the traffic system under cyber-attack?

(2) What is the difference between cyber-attacks on positionand speed?

(3) How sensitive is the traffic system to different cyber-attacked scenarios?

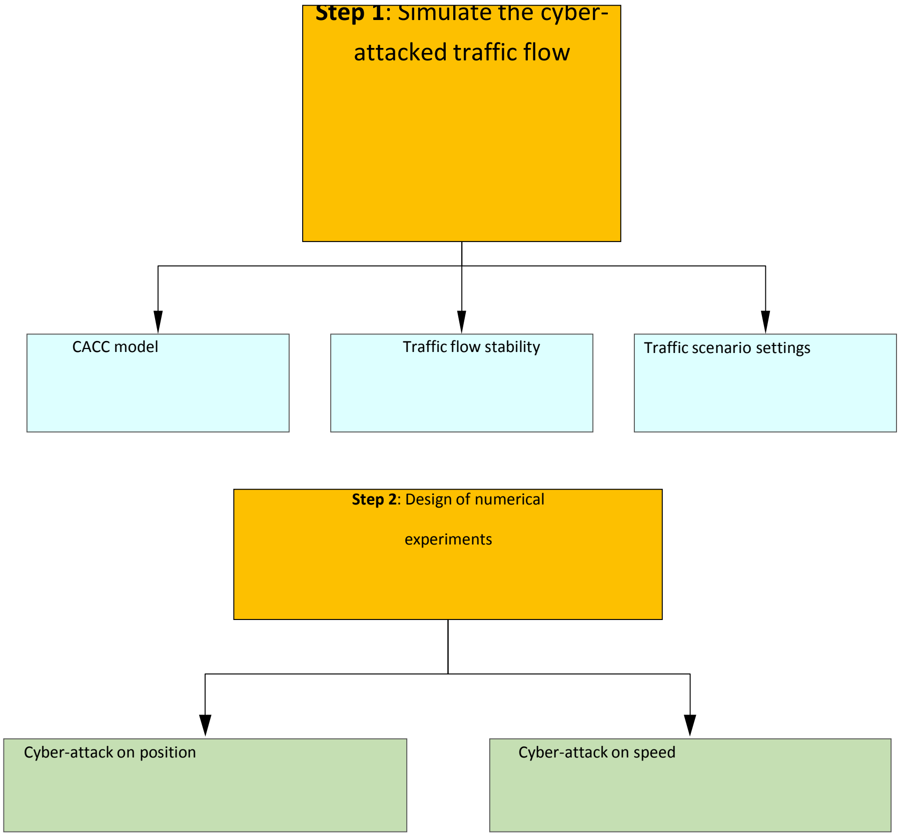
The remainder of this paper is structured as follows: Section II describes the methodology, including the evaluation framework for cyber-attacked traffic and simulation experiment designs. In Section III, the impact of important factors is analyzed, such as object of cyber-attack, proportion of cyber-attacked vehicles, cyber-attack severity. Section IV presents numerical simulation results to indicate the characteristics of the traffic flow under cyber-attack. Sensitivity analysis of cyber-attack range and traffic demand isconducted in Section V. Finally, some conclusions are summarized in Section VI.

2. METHODOLOGY

A. FRAMEWORK

The framework for evaluation of cyber-attack on traffic flow isshown in Fig. 1. It consists of four steps:

- **Step 1:** Model the cyber-attacked traffic flow. To simulate longitude control on CAVs, CACC model is used to characterize the car-following behaviors. Moreover, cyber- attack on traffic flow stability is analyzed from a theoretical perspective, and then traffic scenarios are designed to providea basis for cyber-attack measurement.
- **Step 2**: Based on CACC model and analysis of traffic flow stability, the microscopic simulation testbed is established to imitate potential cyber-attacks on CAVs. Cyber- attacks on position and speed are respectively considered. Also, proportion of cyber-attacked vehicles and cyber-attack severity are selected as independent variables throughout the experiment.
- **Step 3**: Numerical simulations are conducted to display the performance of a basic freeway bottleneck in travel efficiency, traffic safety, emissions and fuel consumption.
- **Step 4**: Cyber-attack range and traffic demand are two important parameters, which the transportation system may besensitive to. Therefore, sensitivity analysis is conducted to investigate their impact on simulation results.


Step 1: Simulate the cyber-attacked traffic flow
CACC model
Traffic flow stability
Traffic scenario settings
Step 2: Design of numerical experiments
Cyber-attack on position
Cyber-attack on speed

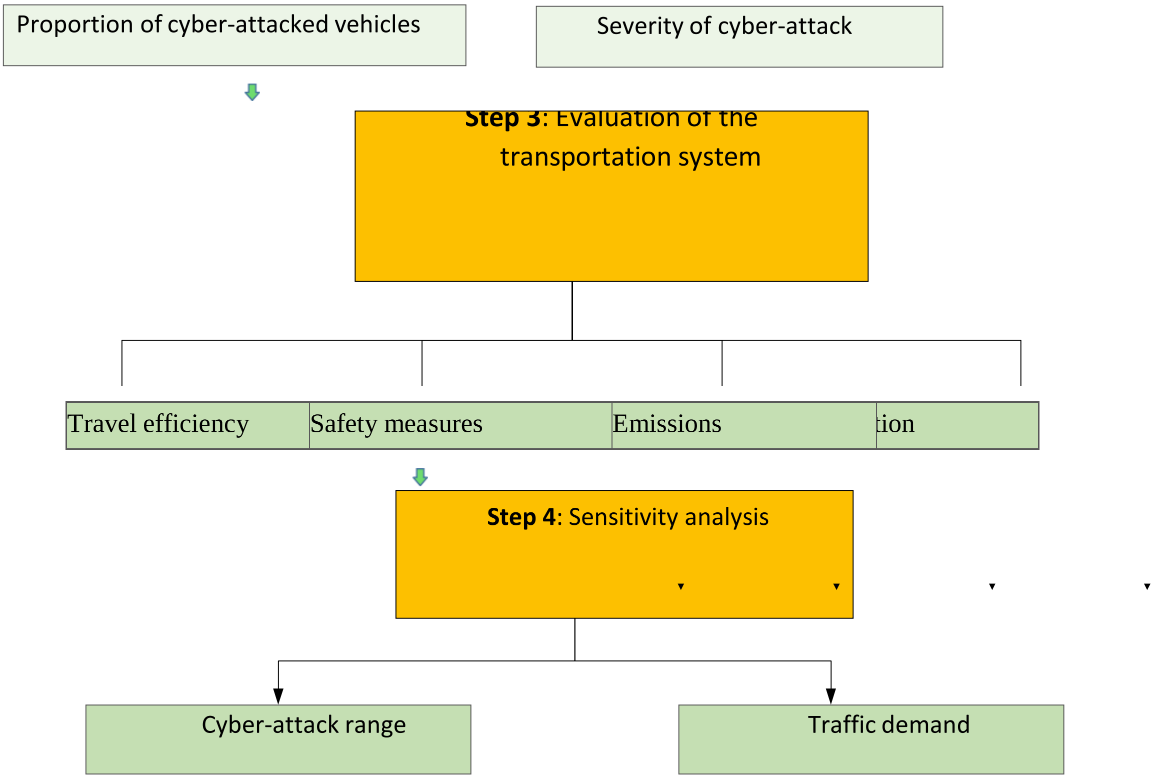
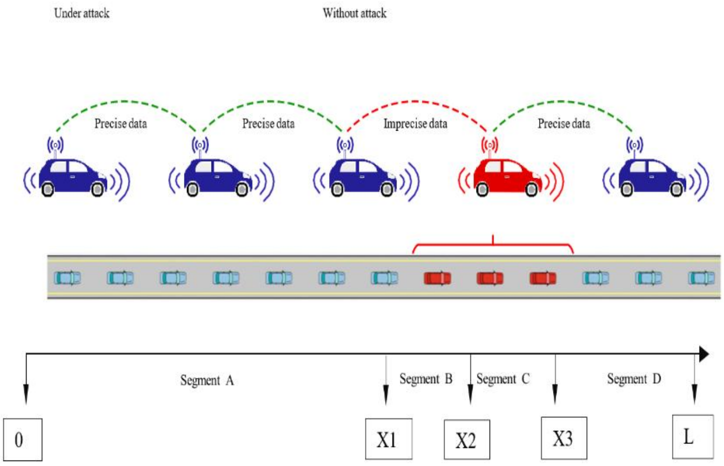

Proportion of cyber-attacked vehicles
Severity of cyber-attack
Step 3: Evaluation of the transportation system
Travel efficiency
Safety measures
Emissions
tion
Step 4: Sensitivity analysis
Cyber-attack range
Traffic demand

Figure 1. Framework of the study.

B. SIMULATION EXPERIMENT DESIGN

The topology structure of communications between CAVsunder or without cyber-attacks is expressed in Fig. 3



C. Functional requirements

Outputs from computer systems are required primarily to communicate the results of processingto users. They are also used to provide a permanent copy of the results for later consultation.

The various types of outputs in general are:

External Outputs, whose destination is outside the organization,.

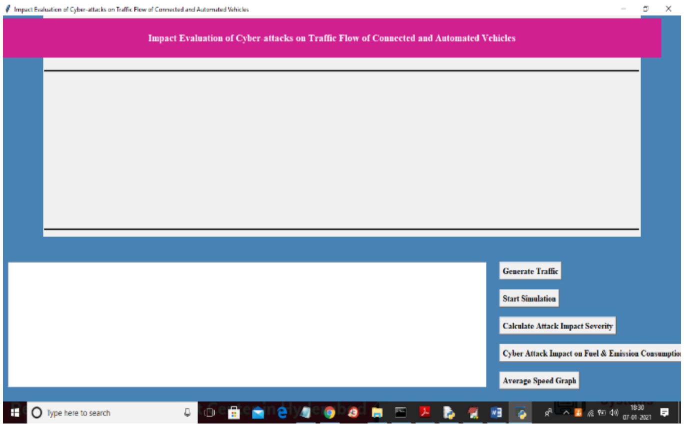
- Internal Outputs whose destination is within organization and they are theuser’s main interface with the computer.
- Operational outputs whose use is purely within the computer department.
- Interface outputs, which involve the user in communicating directly.

Understanding user’s preferences, expertise level and his business requirements througha friendly questionnaire.

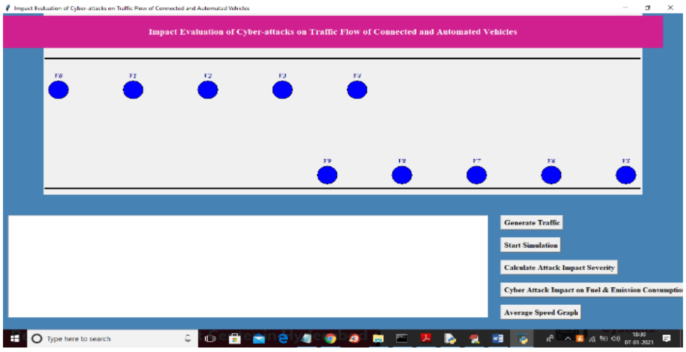
Input data can be in four different forms - Relational DB, text files, .xls and xml files. For testing and demo you can choose data from any domain. User-B can provide business dataas input.

3. RESULT AND DISCUSSION

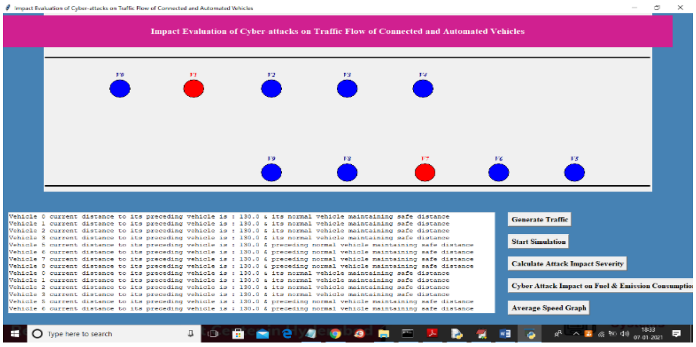
To run project double click on 'run.bat' file to get below screen


Impact Evaluation of Cyber-attacks on Traffic Flow of Connected and Automated Vehicles
Impact Evaluation of Cyber attacks on Traffic Flow of Connected and Automated Vehicles
Generate Traffic
Start Simulation
Calculate Attack Impact Severity
Cyber Attack Impact on Fuel & Emission Consumptio
Average Speed Graph
Type here to search

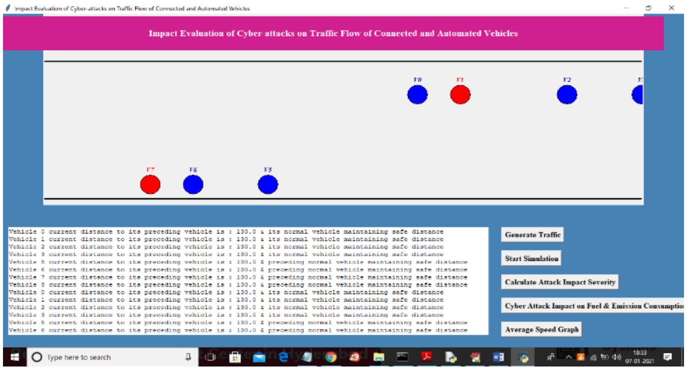
In above screen click on 'Generate Traffic' button to get below screen


Impact Evaluation of Cyber-attacks on Traffic Flow of Connected and Automated Vehicles
Impact Evaluation of Cyber attacks on Traffic Flow of Connected and Automated Vehicles
V0
V1
V2
V3
V4
V9
V8
V7
V6
V5
Generate Traffic
Start Simulation
Calculate Attack Impact Severity
Cyber Attack Impact on Fuel & Emission Consumptio
Average Speed Graph
Type here to search

In above screen we have created traffic with 10 vehicles and each circle will represents one vehicle and now click on 'Start Simulation' button to move vehicles and then intentionally we are injecting some attackers which report fake speed information to nearby vehicles and when two vehicles enter into instable region then vehicle colour will change to red colour and while simulation we can see two vehicles comes to close location due to fake speed

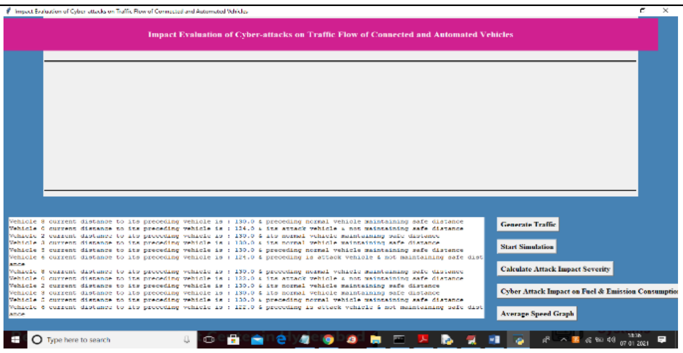

Impact Evaluation of Cyber-attacks on Traffic Flow of Connected and Automated Vehicles
Impact Evaluation of Cyber attacks on Traffic Flow of Connected and Automated Vehicles
V0
V1
V2
V3
V4
V9
V8
V7
V6
V5
Generate Traffic
Start Simulation
Calculate Attack Impact Severity
Cyber Attack Impact on Fuel & Emission Consumptio
Average Speed Graph
Type here to search

```
Vehicle 0 current distance to its preceding vehicle is : 130.0 & its normal vehicle maintaining safe distance
Vehicle 1 current distance to its preceding vehicle is : 130.0 & its normal vehicle maintaining safe distance
Vehicle 2 current distance to its preceding vehicle is : 130.0 & its normal vehicle maintaining safe distance
Vehicle 3 current distance to its preceding vehicle is : 130.0 & its normal vehicle maintaining safe distance
Vehicle 5 current distance to its preceding vehicle is : 130.0 & preceding normal vehicle maintaining safe distance
Vehicle 6 current distance to its preceding vehicle is : 130.0 & preceding normal vehicle maintaining safe distance
Vehicle 7 current distance to its preceding vehicle is : 130.0 & preceding normal vehicle maintaining safe distance
Vehicle 8 current distance to its preceding vehicle is : 130.0 & preceding normal vehicle maintaining safe distance
Vehicle 0 current distance to its preceding vehicle is : 130.0 & its normal vehicle maintaining safe distance
Vehicle 1 current distance to its preceding vehicle is : 130.0 & its normal vehicle maintaining safe distance
Vehicle 2 current distance to its preceding vehicle is : 130.0 & its normal vehicle maintaining safe distance
Vehicle 3 current distance to its preceding vehicle is : 130.0 & its normal vehicle maintaining safe distance
Vehicle 5 current distance to its preceding vehicle is : 130.0 & preceding normal vehicle maintaining safe distance
Vehicle 6 current distance to its preceding vehicle is : 130.0 & preceding normal vehicle maintaining safe distance
```


Impact Evaluation of Cyber-attacks on Traffic Flow of Connected and Automated Vehicles
Impact Evaluation of Cyber attacks on Traffic Flow of Connected and Automated Vehicles
V0
V1
V2
V3
V7
V6
V5
Generate Traffic
Start Simulation
Calculate Attack Impact Severity
Cyber Attack Impact on Fuel & Emission Consumptio
Average Speed Graph
Type here to search

```
Vehicle 0 current distance to its preceding vehicle is : 130.0 & its normal vehicle maintaining safe distance
Vehicle 1 current distance to its preceding vehicle is : 130.0 & its normal vehicle maintaining safe distance
Vehicle 2 current distance to its preceding vehicle is : 130.0 & its normal vehicle maintaining safe distance
Vehicle 3 current distance to its preceding vehicle is : 130.0 & its normal vehicle maintaining safe distance
Vehicle 5 current distance to its preceding vehicle is : 130.0 & preceding normal vehicle maintaining safe distance
Vehicle 6 current distance to its preceding vehicle is : 130.0 & preceding normal vehicle maintaining safe distance
Vehicle 7 current distance to its preceding vehicle is : 130.0 & preceding normal vehicle maintaining safe distance
Vehicle 8 current distance to its preceding vehicle is : 130.0 & preceding normal vehicle maintaining safe distance
Vehicle 0 current distance to its preceding vehicle is : 130.0 & its normal vehicle maintaining safe distance
Vehicle 1 current distance to its preceding vehicle is : 130.0 & its normal vehicle maintaining safe distance
Vehicle 2 current distance to its preceding vehicle is : 130.0 & its normal vehicle maintaining safe distance
Vehicle 3 current distance to its preceding vehicle is : 130.0 & its normal vehicle maintaining safe distance
Vehicle 5 current distance to its preceding vehicle is : 130.0 & preceding normal vehicle maintaining safe distance
Vehicle 6 current distance to its preceding vehicle is : 130.0 & preceding normal vehicle maintaining safe distance
```

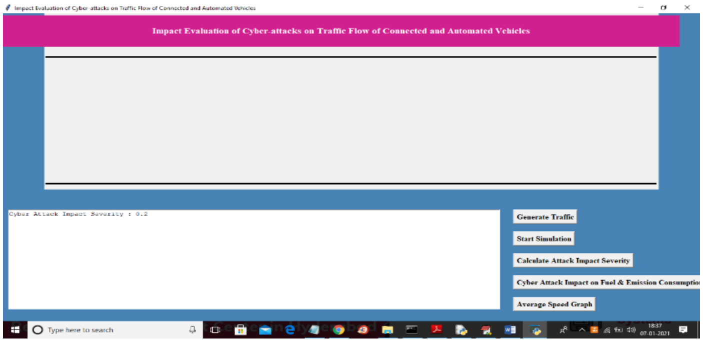
In above screen we can see vehicles start moving in both directions and when vehicle comes too close then it will enter into instable region and red colour preceding vehicle becomes attacker as it report fake speed due to which rear vehicles come too to attack vehicles. In text area also we are displaying distance between current vehicle and its preceding vehicles and also displaying status and once after simulation complete then will get below screen



Impact Evaluation of Cyber-attacks on Traffic Flow of Connected and Automated Vehicles
Impact Evaluation of Cyber-attacks on Traffic Flow of Connected and Automated Vehicles
Generate Traffic
Start Simulation
Calculate Attack Impact Severity
Cyber Attack Impact on Fuel & Emission Consumptio
Average Speed Graph
Type here to search

```
Vehicle 8 current distance to its preceding vehicle is : 130.0 & preceding normal vehicle maintaining safe distance
Vehicle 0 current distance to its preceding vehicle is : 124.0 & its attack vehicle & not maintaining safe distance
Vehicle 2 current distance to its preceding vehicle is : 130.0 & its normal vehicle maintaining safe distance
Vehicle 3 current distance to its preceding vehicle is : 130.0 & its normal vehicle maintaining safe distance
Vehicle 5 current distance to its preceding vehicle is : 130.0 & preceding normal vehicle maintaining safe distance
Vehicle 6 current distance to its preceding vehicle is : 124.0 & preceding is attack vehicle & not maintaining safe dist
ance
Vehicle 8 current distance to its preceding vehicle is : 130.0 & preceding normal vehicle maintaining safe distance
Vehicle 0 current distance to its preceding vehicle is : 122.0 & its attack vehicle & not maintaining safe distance
Vehicle 2 current distance to its preceding vehicle is : 130.0 & its normal vehicle maintaining safe distance
Vehicle 3 current distance to its preceding vehicle is : 130.0 & its normal vehicle maintaining safe distance
Vehicle 5 current distance to its preceding vehicle is : 130.0 & preceding normal vehicle maintaining safe distance
Vehicle 6 current distance to its preceding vehicle is : 122.0 & preceding is attack vehicle & not maintaining safe dist
ance
```

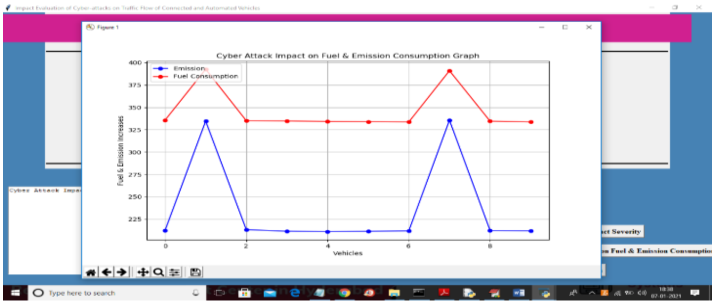
Now click on ‘Calculate Attack Impact Severity’ button to calculate attack severity for this simulation



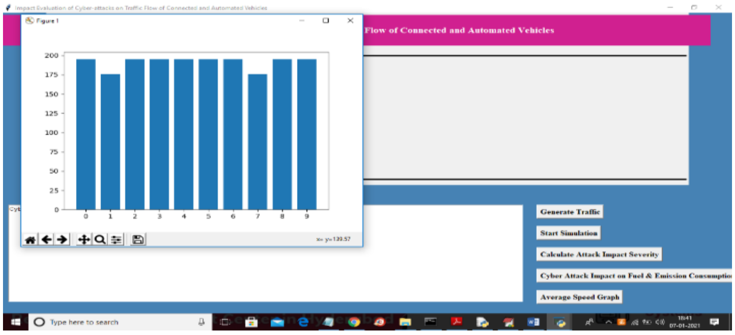
Impact Evaluation of Cyber-attacks on Traffic Flow of Connected and Automated Vehicles
Impact Evaluation of Cyber-attacks on Traffic Flow of Connected and Automated Vehicles
Generate Traffic
Start Simulation
Calculate Attack Impact Severity
Cyber Attack Impact on Fuel & Emission Consumptio
Average Speed Graph
Type here to search

```
Cyber Attack Impact Severity : 0.2
```

In above screen attack severity percentage is 0.2% and now click on ‘Cyber Attack Impact on Fuel & Emission Consumption Graph’ to get fuel and emission consumption between normal and attack vehicles



In above graph x-axis represents number of vehicles and y-axis represents emission or fuel consumption and the vehicle under attack is consuming more fuel and more emission as normal vehicles move in given speed so it’s fuel is same for example in above graph vehicle 2, 3, 4, 5, 6, 8 and 9 is consuming less fuel and other are the attack vehicles which consume more fuel. Now click on ‘Average Speed Graph’ button to get speed graph of all vehicles



In above graph x-axis represents vehicle numbers and y-axis represents speed and then vehicle with less speed consider as attacker as they report fake information and slow down their vehicles which can cause accident to rear vehicles and normal vehicles move with average given speed.So from above experiment we can conclude that impact of cyber-attack on automated vehicles may consume more fuel, emission and cause accidents

4. CONCLUSION

In this paper, we first design the traffic flow simulation experiment for cyber-attacks on CAVs, and then analyze impact of the proportion of attacked vehicles, cyber-attack severity, cyber-attack range and traffic demand. According to the performance on efficiency, safety, emissions and fuel consumption under different traffic conditions, the major results are

concluded as follows:

1. Traffic congestions occur frequently and have significant negative effects on the cyber-attack area when the proportion of attacked vehicles are over 60% under position-attacked conditions. In contrast, the speed-attacked traffic is not sensitive to the proportion of attacked vehicles. The critical values of cyber-attack severity for the position- and speedattacked traffic are respectively 1% and 8%, from which the speeds decline dramatically. Compared with the stable traffic without cyber-attack, the decreases in average speed under speed-attacked conditions are nearly between one-fourth and one-third of that with attacked positions.
2. In the influence area caused by cyber-attack, the safety condition gets worse and leads 2-3 levels than the whole road, especially in the position-attacked scenarios. Moreover, cyberattack causes more 2-20% emissions and fuel consumption with the increase of cyber-attacked vehicles and cyber-attack severity.
3. The longer cyber-attack range caused by the improvement of transmission technology results in more negative effects on traffic efficiency and safety. The average speeds approximately drop by 5 m/s with a 200-meter increase of cyber-attack range.
4. Compared with the traffic below 1500 vph, the 2000-vph traffic demand results in striking decreases and big fluctuations in speeds. In addition,
5. [1000 vph, 2000 vph] is the sensitive range for traffic demand management, where route guidance in advance may be necessary.
6. From the view of attackers, vehicle’s position may be the most potential attack target, and its severity over 1% can cause significant negative effects on travel efficiency and traffic safety. For the defenders, some control methods like VSL can be applied along the influence area for enough reaction time. Additionally, road-side units may send warning massages to CAVs and remind drivers to keep safe distance if unknown attack occurs. There, if the security cannot be guaranteed completely, the control right of CAV should be controlled by the driver to support emergency response.

5. REFERENCES

[1] Dong, H. Wang, Y. Li, W. Wang, and Z. Zhang, “Route Control Strategies for Autonomous Vehicles Exiting to Off-Ramps,” *IEEE Trans. Intell. Transp. Syst.*, pp. 1–13, 2019.

[2] H. Ni, “Determining traffic-flow characteristics by definition for application in ITS,” *IEEE Trans. Intell. Transp. Syst.*, vol. 8, no. 2, pp. 181–187, Jun. 2007.

[3] J. Petit and S. E. Shladover, “Potential Cyberattacks on Automated Vehicles,” *IEEE Trans. Intell. Transp. Syst.*, vol. 16, no. 2, pp. 546–556, Apr. 2015.

[4] C. Y. Dong, H. Wang, Q. Chen, D. H. Ni, and Y. Li, “Simulation-Based Assessment of Multilane

[5] Separate Freeways at Toll Station Area: A Case Study from Huludao Toll Station on Shenshan Freeway,” Sustainability, vol. 11, no. 11, Jun. 1 2019.

[6] C. Wang, C. C. Xu, J. X. Xia, Z. D. Qian, and L. J. Lu, “A combined use of microscopic traffic simulation and extreme value methods for traffic safety evaluation,” Transp. Res. Part C Emerg. Technol., vol. 90, pp. 281–291, May 2018.

[7] Y. Li, H. Wang, W. Wang, L. Xing, S. W. Liu, and X. Y. Wei, “Evaluation of the impacts of cooperative adaptive cruise control on reducing rear-end collision risks on freeways,” Accid. Anal. Prev., vol. 98, pp. 87–95, Jan. 2017.

[8] D. H. Ni, J. D. Leonard, C. Q. Jia, and J. Q. Wang, “Vehicle Longitudinal Control and Traffic Stream Modeling,” Transp. Sci., vol. 50, no. 3, pp. 1016–1031, Aug. 2016.

[9] F. Chen and S. Chen, “Injury severities of truck drivers in single- and multi-vehicle accidents on rural highways,” Accid. Anal. Prev., vol. 43, no. 5, pp. 1677–1688, Sep. 2011.

[10] Y. Li, Z. B. Li, H. Wang, W. Wang, and L. Xing, “Evaluating the

[11] safety impact of adaptive cruise control in traffic oscillations on freeways,” Accid. Anal. Prev., vol. 104, pp. 137–145, Jul. 2017.

[12] Y. Guo, Z. Li, P. Liu, and Y. Wu, “Modeling correlation and heterogeneity in crash rates by collision types using full bayesian random parameters multivariate Tobit model,” Accid. Anal. Prev., vol. 128, pp. 164–174, Jul. 2019.

[13] Y.-Y. Qin, Z.-Y. He, and B. Ran, “Rear-End Crash Risk of CACC- Manual Driven Mixed Flow Considering the Degeneration of CACC Systems,” IEEE Access, vol. 7, pp. 140421–140429, 2019.

[14] C. Xu, J. Ji, and P. Liu, “The station-free sharing bike demand forecasting with a deep learning approach and large-scale datasets,”.