Resilient Cyber-Physical Systems with Application to Vehicle-to-Vehicle Collision Avoidance

Arul Mathi Maran Chandran, Shanshan Bi, Kenneth Naumann, and Jared Hanisch
Missouri University of Science and Technology
Rolla, Missouri 65409-0040

Abstract—**Vehicle-to-vehicle (V2V) communication allows cars broadcast their position, speed, steering-wheel position, brake status, and other data to other vehicles within a few hundred meters. Such wireless technology is likely to improve the safety of self-driving cars. According to the National Highway Traffic Safety Administration, V2V technology could help prevent as much as 80% of accidents and only leaves another 20% to be taken care of by self-driving technology. However, V2V network reliability is not trivial to achieve due to inherent network issues such as delays, packet losses, cyber-attacks, protocol performance, etc. Intelligent vehicles should be aware of such network challenges and avoid catastrophic failures and life-threatening accidents. In this paper, we propose a V2V network fault diagnosis scheme to detect abnormalities in the vehicular network and investigate a fault tolerant decision-making strategy to improve the safety and stability of the entire V2V self-driving car system. The network reliability is studied from the perspective of graph theory and compared it with the performance metrics including throughput, end-to-end delay, and packet delivery ratio, which are obtained using the ns-3 simulator for the same network topology.**

I. Introduction and Motivation

Vehicle accidents result in more than 35-thousands of deaths in the United States [1]. Moreover, it is the leading cause of death for young Americans. One of the solutions for reducing these accidents according to the National Highway Traffic Safety Administration (NHTSA) are connected vehicle systems. Such Vehicle-to-Vehicle (V2V) communication systems are designed to transmit basic safety information between vehicles to facilitate warnings to drivers concerning impending crashes. This technology can also benefit autonomous driving systems by providing timely, and advanced feedback to an accident avoidance mechanism. Moreover, a V2V communication can improve fuel efficiency for the cars by synchronizing cruise control and aid in optimizing autonomous car lane selection. Traffic jams often are caused by a cascading effect of few cars slowing down on a highway that cascades into other drivers slowing down even more and come to stop eventually. Such scenarios can be avoided if the adjacent cars coordinate their adaptive cruise control. Simple proximity sensors or vision systems are effective only with respect to cars directly in front of the particular vehicle. Due to limited sensing horizon, the benefits are also limited and often unrealized as cars have to slow down more than necessary in order to maintain safety margins. In contrast, a V2V network among several cars in a platoon (different cars driving in proximity with similar speed and in the same direction) could extend the benefit and effectiveness of adaptive cruise control to all the nearby cars. However, such V2V-based platoon control is susceptible to disruptions in the V2V network. The network disruptions can be caused by failures in computational and communication (network) components: data corruption, failure of software or hardware, untimely packet delivery, loss of sensor or control communication or cyber-attacks including jamming, eavesdropping, denial-of-service. In particular, if a warning packet delivery is delayed or lost the incoming cars may not be able to slow down in time to avoid traffic jams or crashes. Hence, V2V network reliability is essential for safety and efficiency of such distributed control system. In a broader sense, such connected vehicles would increase safety for drivers, passengers, and pedestrians. Moreover, it will contribute to the smart city concept and efficient evacuation plans during disasters.

Overall, a successful V2V platoon control requires both formation of a reliable overlay service network within the vehicle platoons and coordinated, adaptive cruise control with lane selection that guarantees accident avoidance. The scheme has to take into account the mobility of cars within a platoon, where vehicles join, move through, and leave platoons at random times. Also, the communication has to provide reliable information dissemination in real-time. The envisioned solution would form an overlay network within a vehicle platoon to optimize network performance and an adaptive cyber-physical controller for cruise control at both individual vehicle and platoon levels.

The proposed work aims at understanding and characterize the topology of V2V networks from graph theory perspective (i.e. dynamic networks [2], [3]), the overlay network analysis will be used to develop predictive model which will feed - in real time expected network performance to the cruise control scheme. The expected performance expressed in terms of network delay and packet loss probability distribution functions will in turn be used to identify the safe zone targets for inter-vehicle distance and reference speed. Moreover, a decision-making scheme for line switching will be proposed to maximize traffic flow while maintaining safety and avoiding accidents.

Random synthetic topology scenarios were run in the Python NetworkX [4] to simulate wireless networks and connectivity analysis using graph centrality metrics. The degradation of graph metrics under time-varying topology scenarios was studied. Realistic V2V mobility scenarios using the ns-3 [5] network simulator mobility models were run to study dynamic routing in V2V scenarios to understand the impact of realistic constraints such as delay and connectivity. Using a V2V example, larger, distributed, and mobile cyber-physical systems were modeled. The model should able to provide insight into the potential benefit of a wider horizon of control feedback and challenges due to network dynamics and failures.

II. V2V Overlay Networks and Graph Theory

There have been many graph metrics to study and improve network performance. In this study, we focus on graph centrality metrics. Closeness centrality describes how close a node is to all other nodes in terms of shortest paths. It is measured as a reciprocal of farness. The farness is the sum of the shortest paths from a particular node to all other nodes in the network [6]. As the sum of the distances from all other nodes depends on the number of nodes in the network, closeness centrality is normalized with $n-1$. Betweenness is the number of shortest paths that go through a node or a link [6]. This metric describes how central a node is, compared with all other nodes in the network. It is normalized by the ratio of shortest path through a node or through an edge over the total number of shortest paths in that network. Finally, algebraic connectivity is the second smallest eigenvalue of the Laplacian of a given graph G [7]. Its value is bounded by 0 if the graph is disconnected, and maximum value depends on the number of nodes and how these nodes are connected.

Consider an example of a national backbone network and which needs to be expanded for the mobile and wireless scenarios of V2V communications. The characteristics of V2V scenarios include: a group of cars moving as a platoon. The Manhattan grid and highway mobility models [8] are realistic models to study the performance of V2V communications. A second aspect is the when there are no direct line-of-sight links between vehicles, how to intelligently decide to route the packets between end points. An alternative is to utilize the existing vehicular communication apparatus as an underlay and having an overlay to provide multihop routing. Thus, the second aspect is to develop network models to study graph properties such that the safety-critical information can be communicated between vehicles. An important third aspect is looking into realistic constraints such as lack of connectivity, number of vehicles in group communication, delay, and interference caused by the surrounding vehicles. Thus, the impact of realistic constraints will be studied under the dynamic routing schemes so that their impact can be understood.

III. Resilient, Stochastic Network Control for Connected Vehicles

In the past few years, many control and system researchers have pioneered the development of approaches and tools to model and control CPSs. [9], [10], [11], [12], [13] addressed the fault detection, isolation, and mitigation in the physical subsystem alone (e.g. actuators, sensors, and controlled components). They assumed the network performs well and satisfies their prior assumptions. Therefore, the interactions between cyberspace and physical world are ignored or simplified.

A one-class support vector (OCSV) machine based network diagnosis scheme was proposed to detect the cyber network faults. In case of V2V-based cruise control, the network faults are defined as delay and packet losses that exceed safety margins in particular, if the feedback latency increases such that the probability of rear-ending a car the exceeds acceptable level. The model of cyber dynamics (time delay and packet loss) and car speed, acceleration, and path selection is proposed [14] [15]. The performance of OCSV will be evaluated in simulations. Fig. 1 and Fig. 2 illustrate the proposed cyber-physical scheme to be employed for the V2V scenario.

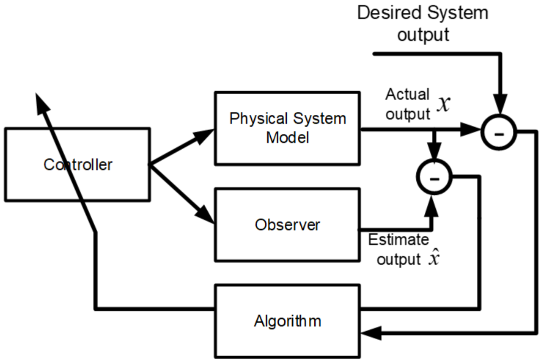

Fig. 1: Tolerant control for physical system fault

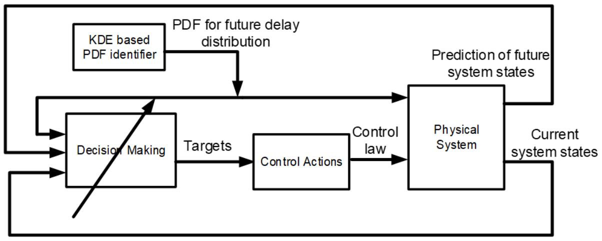

Fig. 2: Resilience solution

A novel diagnosis scheme is shown to quickly detect and isolate cyber network faults using PDF monitoring and estimation. With the proposed resilience controller, the adverse effects caused by cyber network faults are effectively mitigated. The stability of the proposed controller is proved using Lyapunov-based analysis.

IV. Scenarios and Results

In this section different vehicular networks are discussed to describe the effect of delay variation in the network and also relate results from the ns-3 network simulation and theoretical graph results generated using the NetworkX. The theoretical graph results can provide insight into the theoretical limit of the network performance and can be correlated with the results from the ns-3 simulation results.

A. Cybersecurity for Vehicular Network Application

Car S is a self-driving car and other cars have human drivers. Car S should keep a proper speed and vehicle distance to track Car 2 and avoid a car crash. If the network condition is perfect, the information between Cars 2 and S can be delivered within 0.2 s which is faster than vision-based detection 0.6 s, and their vehicle distance should be 15 meters to guarantee Car S can stop safely when a crash happens on Cars 1 and 2 (Fig. 3, (a)). When a network congestion happens, the delay increases from 0.2 s to 0.4 s. Therefore, the vehicle distance between Cars 2 and S should be longer to allow more time to receive the information about emergence.

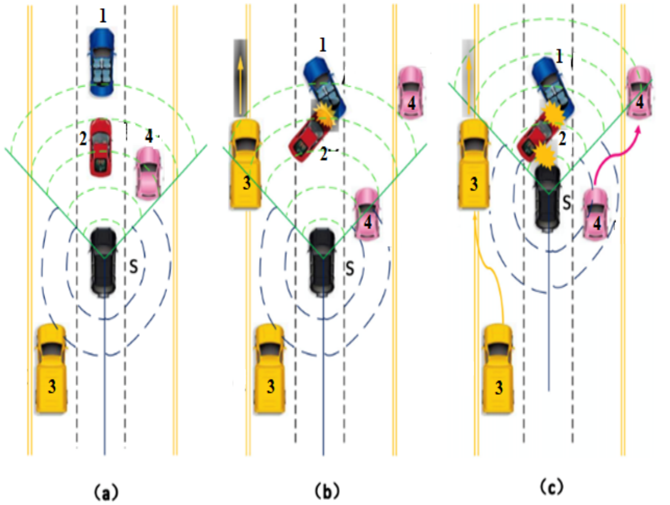

Fig. 3: Example vehicular network scenario

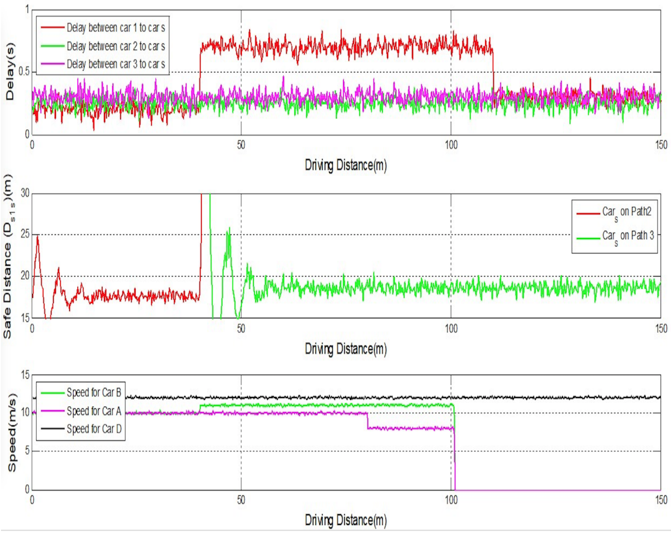

Fig. 4: Resilience control of collision avoidance system

If their distance is not adjusted depending on the delays, Car S might hit the back of Car 2 when a car crash happens on Cars 1 and 2 (Fig. 3. (c)). It is concluded that network faults indeed affect the safety and reliability of self-driving cars. We evaluated a simple scenario where five cars drive on a high way, as shown in Fig. 1. A cyber fault occurring at 40 s, where the average network delay increases from 0.2 s to 0.7 s. Also, the distance between 1 and 2 doesnt meet the required safe distance. As a result, the self-driving car (S) would have to significantly increase the distance to next car effectively causing it to stop and start a traffic jam. Our proposed resilience scheme would provide the safe targets for the cruise control. But it also can be used to evaluate adjacent paths. In the presented simulation (Fig. 4), car S could switch from Path 2 to Path 3 to reduce the probability of accident while maximizing driving speed.

B. Analysis of Graph and Network Simulation

In this section, we discuss the example scenario of cars with simple network topology. The results from the NetworkX [4] and the ns-3 [5] are compared and analyzed for more insight to understand how the results from graph analysis used for larger network independent of the protocols used. Fig. 5 shows the topology of cars which was analyzed using both the NetworkX and the ns-3.

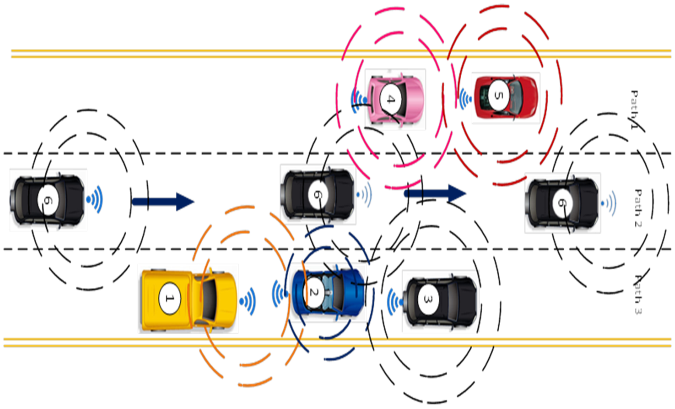

Fig. 5: Example network topology of cars

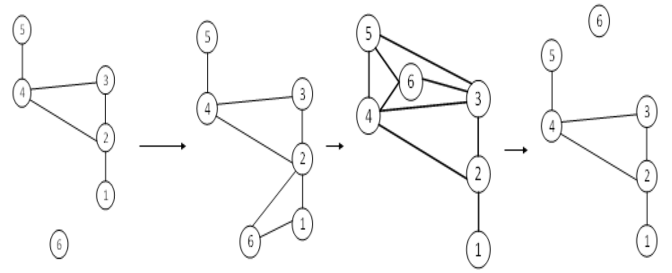

Fig. 6: Transition of adjacency over time

Six cars 1-6 forms the network where the speed of cars 1, 2, 3, 4, and 5 are same, whereas car 6 is faster compared to others. Cars 1, 2, and 3 are in the rightmost lane, and cars 4 and 5 are in leftmost lane. Car 6 passes the other cars through the middle lane. The transmission range around the cars is fixed (5 m) and cars 1, 2, 3, 4, and 5 form the initial network topology, whereas car 6 joins the network at the time, t = 10 s and leaves the network at t = 34 s. All the cars generate data packet of length 512 bits for every 15 ms. Different trials with different data rate are simulated and correlated their results. The data flow between the cars are selected at random and it can hop across multiple nodes. AODV routing protocol was used in the ns-3 simulation since it also considers the shortest path between the nodes similar to that of the graph metrics considers for correlation, and also provides a reasonable performance and adapts well for driving at high-speed vehicular network [16].

Fig. 6 illustrates the changing edges across the nodes in the graph due to change in adjacency nodes across the duration of the simulation. Movement of car 6 affects the topology of existing network when it arrives and keeps altering the links until it leaves the network formed by cars 1 to 5. The adjacency matrix at each time instance was generated and saved to a file, which is used by NetworkX to analyze the network as a graph and generate different graph metrics such as node betweenness, algebraic connectivity, node closeness, clustering coefficients, edge betweenness, shortest path, etc,.

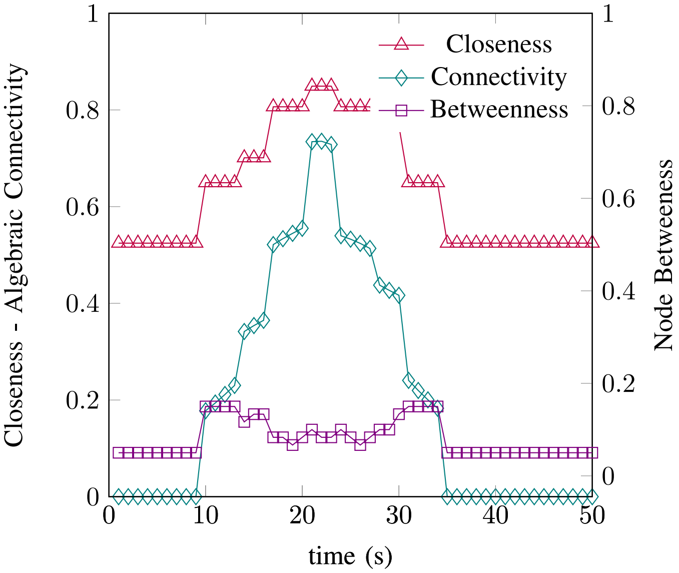

Fig. 7: Graph metrics calculated for the give network topology at each instant of time

Fig. 7 shows the different unweighted graph metrics such as closeness, algebraic connectivity, and betweenness, computed at every second of the simulation using the NetworkX, and its corresponding network performance, throughput is shown in Fig. 8 which generated using the ns-3 simulation.

The maximum, average, and minimum throughput among the six flows generated by the network at every second when operated at 68 kbps throughput are shown in the Fig. 8. The considered throughput of 68 kbps offers moderate capacity demand for the given scenario. When the car 6 approaches the cars, the flows from and to car 6 are initiated altering the existing network topology. As the car 6 moves, it forms and drops links with the other cars which results in AODV reroute. Flooding occurs during AODV reroute which can be observed from the fluctuations in maximum throughput plot from Fig. 8. Once the car 6 leaves the other cars and no more change to the links across the cars, the throughput stabilizes and can be observed from time, t = 35 s. The minimum throughput plot shows the data flow to and from car 6 when it passes the other cars.

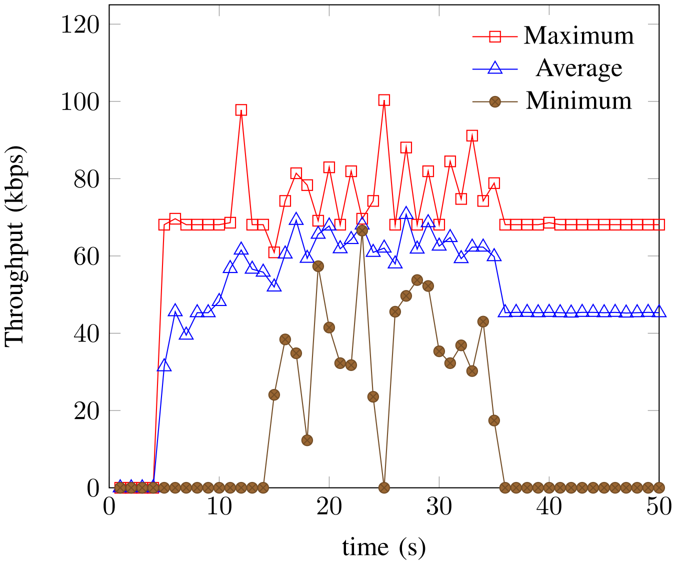

Fig. 8: Throughput comparison

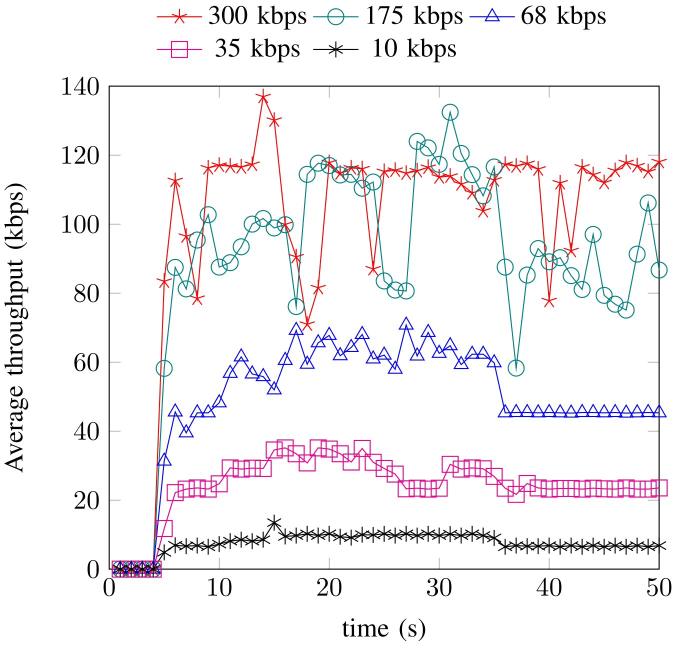

Fig. 9: Comparison of average achieved for different data rates

The ns-3 simulation was run with different source data rate such the congestion at the nodes across the network is varied and studied the impact on network performance. Fig. 9 shows the average throughput of the network at every second of the simulation for different data rates such as 10 kbps, 35 kbps, 68 kbps, 175 kbps, 300 kbps. It can be observed from Fig. 9 that the average throughput of the network stays near data rate for moderate data rates such as 68 kbps, 35 kbps, and 10 kbps, whereas the average throughput drops for higher source data rate. This is due to congestion at nodes which lead to drop/loss of packets and also the inability of the routing scheme to keep up with the altering network leads to failure of links across the nodes resulting in loss of packets.

Similar study was done with distance weighted graph metrics. The unweighted metrics are generated using the adjacency matrix of the nodes in the graph which is a binary matrix, whereas the distance weighted metrics are generated using the product of the adjacency matrix and the distance matrix of the graph. The weights are inversely proportional to the distance between the nodes and distance weighted plot provide more realistic link metric between the nodes in the graph. Similarly, weights using distance matrix can use the other metrics such as closeness and algebraic connectivity.

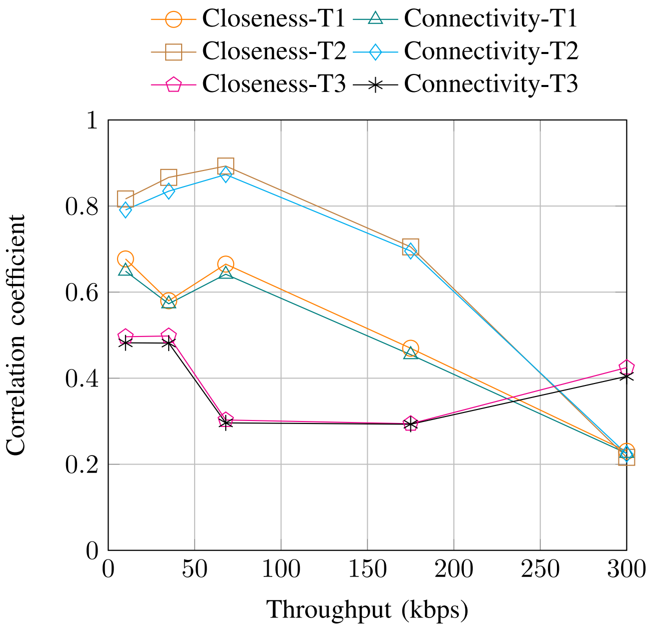

Fig. 10: Correlation coefficients for trials with different random flows between the cars - Closeness, Algebraic Connectivity

The correlation between the graph metrics such as closeness, algebraic connectivity, and betweenness with the network performance metric throughput was studied for the considered network topology. The average throughput across the different flows in the network is correlated with the graph metrics. Fig. 10 shows the correlation coefficients between closeness, algebraic connectivity and average throughput for different trials where the pairs in the network were changed in addition to the different data rates are the source nodes. It can be observed the correlation coefficients of both closeness and algebraic connectivity have similar plots with average throughput since they relate to the shortest path between nodes indicating higher throughput. Similarly, as the source data rate increases which increase the congestion where the packets penalized in a longer path through the nodes. The overall correlation coefficients of trail 3 are lower compared to trial 1 and 2 is due to lack diversity in the nodes interacting in the network. In trial 3, almost all the nodes are communicating to one single node which reduce the diversity of the network interaction. The graph metrics captures the complete possibility of network interaction and each simulation result is a subset. In case of a vehicular network, all cars broadcast and interact with all other cars on the road, so higher correlation with the graph metric predictions is maintained.

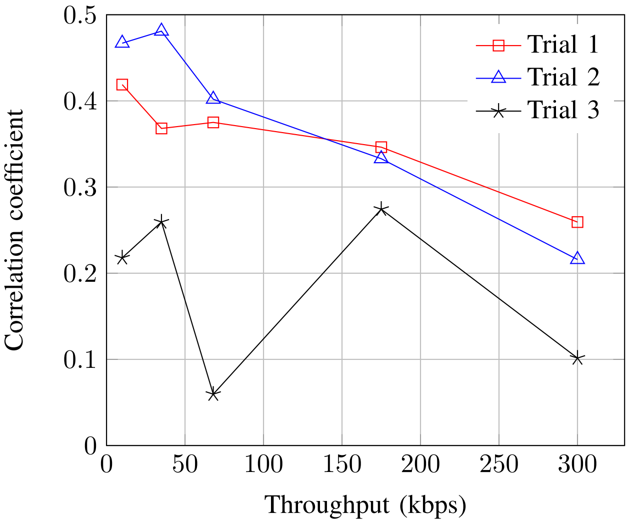

Fig. 11: Correlation coefficients for trials with different random flows between the cars - Betweenness

Fig. 11 shows the correlation coefficients between betweeness and average throughput for different trials where the pairs in the network were changed in addition to the different data rates are the source nodes. It can be observed that the correlation coefficients are low compared to the correlation coefficients shown in Fig. 10. This is expected since the betweenness indicates the number of shortest path through a given node which is more relatable to the congestion at the nodes. In addition, the indication of the impact on the network throughput and used as a composite metric with other graph metrics to estimate maximum bound of achievable throughput.

V. Conclusion

Incipient detection of cyber faults allows improved decision making. In case of a vehicular network, timely detection and resilience prevent collisions and a highly resilient network can handle channel distortions and interference to maintain the desired throughput ensuring timely delivery of data packets.

The graph metrics such as closeness and algebraic connectivity have a high correlation with the average throughput of the network when the congestion at the nodes in the network are moderate. Thus, graph metrics can be employed to predict the network performance which allows characterizing the reliability of a given network.

The future works will be on the proposal of a mathematical model to relate graph metrics of a given topology to actually network, enabling us to analyze and predict network performance of large networks which is difficult to characterize using network simulations. Graph metrics can also provide overall bound of the network performance irrespective of the protocols used by the network. We will investigate other graph metrics such as graph spectra and graph energy and how the graph connectivity degrades with the node/link removals in these dynamic scenarios.

Acknowledgment

The authors would like to thank Dr. Maciej Zawodniok and Dr. Egemen Çetinkaya for their support and guidance throughout this project.

References

[1] "USDOT Releases 2016 Fatal Traffic Crash Data." [Online]. Available: https://www.nhtsa.gov/press-releases/usdot-releases-2016-fatal-traffic-crash-data

[2] D. Zhang, S. A. Gogi, D. S. Broyles, E. K. Çetinkaya, and J. P. Sterbenz, "Modelling Attacks and Challenges to Wireless Networks," in *Proceedings of the 4th IEEE/IFIP International Workshop on Reliable Networks Design and Modeling (RNDM)*, St. Petersburg, October 2012, pp. 806–812.

[3] T. A. Shatto, K. L. Kosbar, and E. K. Çetinkaya, "Graph Theoretic Modeling and Energy Analysis of Wireless Telemetry Networks," in *Proceedings of the International Telemetering Conference (ITC)*, Las Vegas, NV, October 2017.

[4] "Python NetworkX library." [Online]. Available: https://networkx.github.io

[5] "Network Simulator NS3." [Online]. Available: https://www.nsnam.org

[6] L. C. Freeman, "A Set of Measures of Centrality Based on Betweenness," *Sociometry*, vol. 40, no. 1, pp. 35–41, 1977.

[7] M. Fiedler, "Algebraic connectivity of graphs," *Czechoslovak Mathematical Journal*, vol. 23, no. 2, pp. 298–305, 1973.

[8] "Mobisim: Manhattan Mobility Model." [Online]. Available: http://masoudmoshref.com/old/myworks/documentpages/mobisim/manhattan.html

[9] F.-C. Liu and Y. Yao, "Modeling and analysis of networked control systems using hidden markov models," in *2005 International Conference on Machine Learning and Cybernetics*, vol. 2, Aug 2005, pp. 928–931 Vol. 2.

[10] G. P. Liu, Y. Xia, J. Chen, D. Rees, and W. Hu, "Networked predictive control of systems with random network delays in both forward and feedback channels," *IEEE Transactions on Industrial Electronics*, vol. 54, no. 3, pp. 1282–1297, June 2007.

[11] H. Zhang, J. Yang, and C. Y. Su, "T-s fuzzy-model-based robust h infinity; design for networked control systems with uncertainties," *IEEE Transactions on Industrial Informatics*, vol. 3, no. 4, pp. 289–301, Nov 2007.

[12] Y. Wang, H. Ye, and G. Wang, "A new method for fault detection of networked control systems," in *2006 1ST IEEE Conference on Industrial Electronics and Applications*, May 2006, pp. 1–4.

[13] Z. Zhang-qing and Z. Xian-zhong, "Fault detection based on the states observer for networked control systems with uncertain long time-delay," in *2007 IEEE International Conference on Automation and Logistics*, Aug 2007, pp. 2320–2324.

[14] S. Bi and M. Zawodniok, "PDF-based tuning of stochastic optimal controller design for cyber-physical systems with uncertain delay dynamics," *IET Cyber-Physical Systems: Theory Applications*, vol. 2, no. 1, pp. 1–9, 2017.

[15] ——, "A Novel Cyber Network Fault Diagnosis Scheme for Cyber-Physical Systems," in *2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, June 2017, pp. 30–36.

[16] S. S. Kang, Y. E. Chae, and S. Yeon, "Vanet routing algorithm performance comparison using ns-3 and sumo," in *2017 4th International Conference on Computer Applications and Information Processing Technology (CAIPT)*, Aug 2017, pp. 1–5.