Data-Driven Abnormal Behavior Detection for Autonomous Platoon

Seyhan Ucar*, Sinem Coleri Ergen† and Oznur Ozkasap*
Department of Computer Engineering*
Department of Electrical and Electronics Engineering†
Koc University, Istanbul, Turkey
{sucar, sergen, oozkasap}@ku.edu.tr

***Abstract*—Autonomous platoon is a technique where cooperative adaptive cruise control (CACC) enabled vehicles are organized into groups of close following vehicles through communication. It is envisioned that with the increased demand for autonomous vehicles, platoons would be a part of our life in near future. Although many efforts have been devoted to implement the vehicle platooning, ensuring the security remains challenging. Due to lack of security, platoons would be subject to modified packets which can mislead the platoon and result in platoon instability. Therefore, identifying malicious vehicles has become an important requirement. In this paper, we investigate a data-driven abnormal behavior detection approach for an autonomous platoon. We propose a novel statistical learning based technique to detect data anomalies. We demonstrate that shared speed value among platoon members would be sufficient to detect the misbehaving vehicles.**

I. Introduction

Advances in the automobile industry and urbanization make vehicles connected with each other as well as city infrastructure. Not only business plans are changing due to connected and urbanized lifestyle, but also transportation is becoming more intelligent with smart roads that connect smart cars. While these smarter vehicle technologies are in progress, the combined function of automation such as CACC comes into the reality where autonomous vehicles cruise themselves by accessing each other's information.

CACC is an extension to the adaptive cruise control (ACC) systems where short distance automatic following is enabled using inter-vehicular communication. Vehicle platooning, on the other hand, is a technique where CACC enabled vehicles are organized into groups of close following vehicles called platoons [1]. It is predicted that the platoons will behave much better than drivers allowing to handle more traffic with lower delays by traveling with small speed/distance variation, less pollution via preventing unnecessary acceleration/deceleration and better driver/passenger comfort and safety through faster response to events than drivers. With these significant improvements, many researchers have shown great interest in platoon where the California Partners for Advanced Transportation Technology (PATH) demonstrates that platoons produce a significant increase in the capacity of both highway and urban roads to meet the increasing travel demand with a minimum new infrastructure construction [2].

A platoon consists of a leader and follower vehicles where platoon followers follow the leader via adjusting the speed. Platoon stability is one of the significant objectives that platooned vehicles need to achieve [3]. A platoon is said to be stable if the platoon followers utilize CACC to adjust the speed and distance to the leader in terms of variation over time. To ensure the platoon stability, many studies have been proposed to make such an autonomous system practically works [3]–[6]. Platoon systems usually adopt the current dominant vehicular radio frequency technology IEEE 802.11p. Although the high transmission range of IEEE 802.11p provides access to a large number of vehicles at once, the wide coverage makes this communication technology vulnerable to adversaries blocking and interrupting the communication among the vehicles.

Despite many efforts have been devoted to implement the vehicle platooning, ensuring the security remains challenging. Due to lack of security, platoons can be subject to modified packets from malicious vehicles which misleads the platoon members and results in platoon instability [7]. Although certificate based approaches may solve the instability from outsider attackers that are not part of the platoon, the case where the adversary is trusted insider such as compromised platoon members with a valid certificate is still problem [8]. Typical approaches to handle this problem require misbehavior/anomaly detection techniques. Therefore, efficiently identifying those modified packets and insider misbehaviors has become an important requirement in securing autonomous platoon.

Trust management is one of the techniques proposed in Vehicular Ad Hoc Networks (VANETs) to detect misbehaving vehicles by establishing a trust model with a reputation mechanism [9]. Vehicles perform trust model construction and vote against the event. The goal of trust management is to allow each vehicle in a VANET to detect misbehaving vehicles as well as malicious data sent by these dishonest vehicles and to use the data that is generated from vehicles which are behaving honestly. Trust model construction can be divided into three categories; entity oriented, data-driven and combined [10]. Entity oriented trust models focus on modeling the trustworthiness of vehicle itself. The trustworthiness of data has been concentrated on data-driven trust models where vehicles use specific events to evaluate the trustworthiness. Combined trust models, on the other hand, target both the vehicle's trust and the trustworthiness of events.

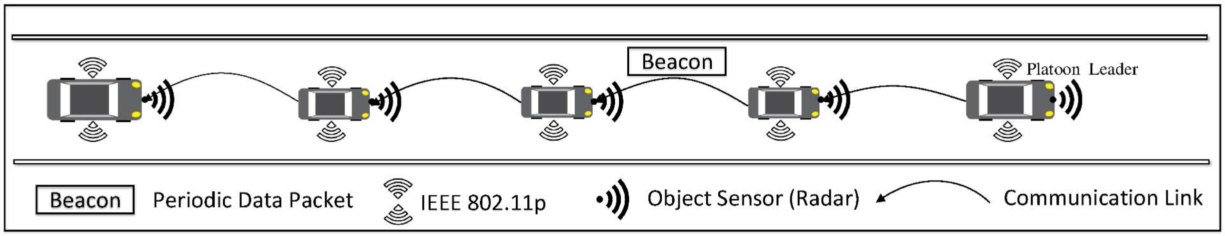


Fig. 1: Platoon System Model

It is shown that data-driven trust model is more suitable for VANET [11]. The trust value is computed based on predefined events [12]–[15]. However, these data-driven approaches are not directly applicable to platoons and have three problems. First, trust value of the vehicle depends on the availability of resources such as the map or density information where these resources may not be as a standard accessory of all autonomous vehicles. Second, the data-driven trust models suffer from the event sparsity where it is difficult and misleading to calculate the trust value. Due to event sparse environment, platooned vehicles cannot distinguish between a rogue and an honest vehicle. Third, data-driven models include Road Side Units (RSUs) as a solution to event sparsity and resources dependency. However, the usage of this scheme in vehicle platoons has the following drawbacks. First, the communication with the RSUs can create a single point of failure, making it vulnerable to several attacks. Second, the large communication overhead and delay associated with the trustworthy of data for each packet is not tolerable in time-critical vehicle platoons.

In this paper, we investigate the data-driven abnormal behavior detection algorithm for an autonomous platoon. The original contribution of this paper is threefold. First, we propose a novel statistical learning based technique to detect data anomalies in the autonomous platoon. Second, the proposed algorithm utilizes only the shared speed values to detect misbehaving vehicles without the usage of any events or RSU. Third, we discuss the alternative ways to alleviate the effect of the misbehaving vehicles.

The rest of the paper is organized as follows. Section II describes the platoon model and misbehaving vehicle's characteristics. Section III presents the proposed data-driven abnormal behavior detection algorithm. Section IV provides the performance evaluation of platoon in the presence of misbehaving vehicles. Finally, conclusions and future work are given in Section V.

II. System Model

A. Platoon Model

Fig. 1 represents IEEE 802.11p communication enabled platoon model. Platoon members use object sensors to detect the object and vehicles in front. IEEE 802.11p is used for communication between vehicles. Each vehicle cooperatively exchanges messages with its preceding and following vehicles via sending the packet from IEEE 802.11p to achieve the CACC. Platoon communication refers to the dissemination of beacon message to the platoon members. Beacon message contains platoon identifier, the speed, position, acceleration of the platoon leader and is periodically disseminated to the platoon followers. From platoon stability perspective, beacon message needs to be delivered to the followers without any disturbance. Upon reception of the beacon messages, platoon member adjusts its own speed and distance to the preceding vehicle based on the speed and acceleration information of the vehicle itself and the preceding vehicle. The goal of this speed and distance adjustment is to keep a safe space gap to the vehicle in front. The vehicle then updates the sender address, speed and acceleration fields in beacon message and sends it to the following vehicle.

B. Misbehaving Vehicle Characteristics

Misbehaving vehicles aim to destroy platoon stability by modifying the beacon message. The attacker vehicles are assumed to be a vehicle in the platoon (either a platoon follower or a leader). The adversary is considered as an honest vehicle by other platoon members. However, upon receiving a beacon message, the adversary alters the content and rebroadcasts. The re-broadcasted beacon message contains wrong information which misleads the platoon members and degrades the platoon stability. For instance, consider a scenario where misbehaving vehicle changes the acceleration of platoon from slowing down to speeding up. Modifying the acceleration may result in a collision.

III. Data-Driven Abnormal Behavior Detection Algorithm

To detect the data anomalies, we propose a novel statistical learning based technique. The unique features of the proposed approach are; it uses only the speed values to detect misbehaviors, it employs time series decomposition to detect speed anomalies.

```
Algorithm 1: Anomaly Detection
1 Split the speed observations $X$ into chunks $C_X$;
2 foreach $C_X$ do
3     Extract seasonal $S_X$ component using STL;
4     Compute median $\widetilde{X}$;
5     Compute residual $R_X = X - S_X - \widetilde{X}$;
6     $X_A = ESD(R_X, N_V)$;
7     Add $X_A$ to speed anomaly vector $v$;
8 Return $v$;
```

Algorithm 1 is run on vehicle's speed values to detect data anomalies. The algorithm starts by splitting speed data X into non-overlapping chunks C_X containing at least two observations (Line 1). Following that, for each C_X, the anomaly detection algorithm is executed. (Lines $2 - 7$). The anomaly detection starts with decomposition based on Seasonal and Trend decomposition using Loess (STL) [16] (Lines $3 - 5$). STL is a technique that decomposes the X into three components; seasonal (S_X), trend (T_X) and residual (R_X). The seasonal component describes the periodic variation of the speed observations, whereas the trend component describes the long-term non-periodic variation. The residual component, on the other hand, is defined as $R_X = X - S_X - T_X$ where the seasonality and trend have been removed from the speed observations.

Typical anomaly detection algorithms use the sample mean and standard deviation to detect an anomaly in input data. However, the distortion of the mean increases as the time goes infinity [17]. The proposed approach, on the other hand, uses the median, which is robust against such anomalies [18]. After decomposition and median calculation, the Generalized Extreme Studentized Deviate (ESD) is run on R_X to detect possible outliers (Line 6). The ESD is an outlier detection technique that is used to detect anomalous observations in sample data [19]. The ESD takes the parameters the residual speed observations and the upper bound on the number of potential outliers which is the number of vehicles in a platoon, N_V. After ESD execution, the speed anomaly, X_A, is detected and it is added to the speed anomaly vector, v (Lines $6 - 7$). X_A consists of the simulation time and the abnormal speed value that are detected by ESD. After all C_X evaluation, speed anomaly vector, v, is returned as the output (Line 8).

In Algorithm 1, STL filters the seasonal and trend components from the raw data. It has been shown that applying ESD on seasonal or trend data is highly susceptible to the presence of anomalies and it most likely introduces artificial anomalies [20]. The analysis here uses only the residual component of speed observations with predefined chunk size. As part of future research, we plan to conduct analysis by considering the seasonal and trend components of data in different chunk sizes.

IV. Performance Evaluation

The goal of the performance evaluation is to detect the misbehaving vehicles and speed anomalies in the platoon. The IEEE 802.11p is used for the communication among vehicles. The speed value observations are collected via the simulation in VEhicular NeTwork Open Simulator (VENTOS) [21] and these speed value observations are analyzed with R [22] separately. VENTOS is a simulator integrating realistic mobility generator, Simulation of Urban Mobility (SUMO) [23]; the discrete packet-level simulator, OMNET++ [24]; and vehcile-to-vehicle (V2V) communication platform, Vehicles in Network Simulation (Veins) [25]. R, on the other hand, is a programming language and software environment for statistical analysis, graphics representation and reporting. Time series decomposition and outlier detection mechanisms of proposed anomaly detection algorithm adopt STL and ESD from R, which is provided from an open access library.

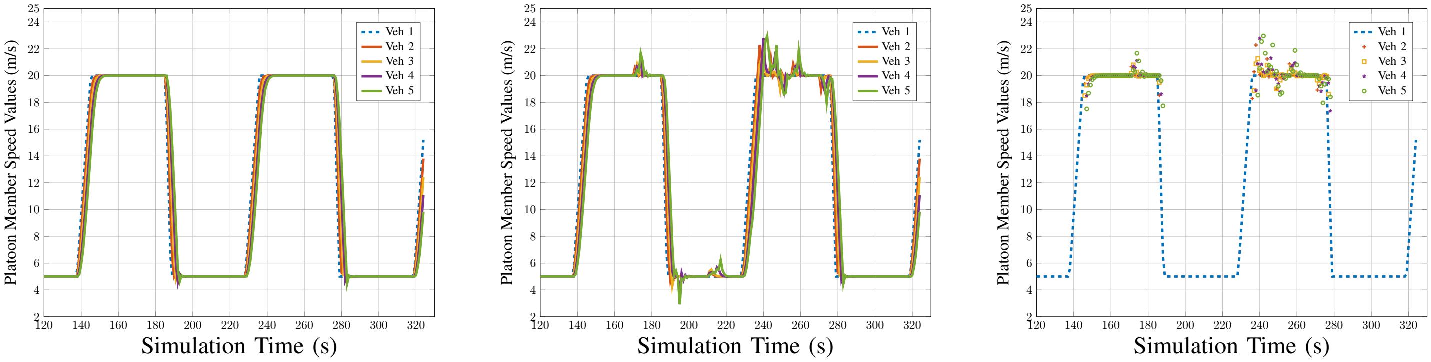
In VENTOS, simulated road topology consists of a two-lane road of length 90 km with the leftmost lane reserved for platooned vehicles. The vehicles are injected into the road from the right lane according to Poisson process at 0.5 vehicles per second rate. CACC enabled vehicles move to the leftmost lane to form a platoon. A platoon consists of 5 autonomous vehicles. $Vehi$ refers to the $i - th$ vehicle in the platoon, with $Veh1$ as the first vehicle. The first vehicle $Veh1$ is referred as a platoon leader and shown with a dashed blue line in the graphs. The mobility of the platoon leader depends on the road speed limit, that varies between 5 and 20 m/s. Platoon followers adjust their speed based on the exchanged beacon messages via wireless communication with the goal of tracking the speed of the leader vehicle and keeping a constant inter-vehicular space gap. In the simulation, the leader, $Veh1$, is misbehaving where it manipulates the speed and acceleration fields of beacon message between the times at t = 172 s and t = 280 s to ruin the platoon stability. For each vehicle, 205 speed observations are collected and analyzed with R. Apart from these, Table I lists other parameters.

TABLE I: Parameters

	Parameter	Value
Simulation	Simulation Time	325 s
	Vehicle Length	5 m
	Number of Vehicles	5
	IEEE 802.11p Range	300 m
	Communication Frequency	10 Hz
	Chunk Size	10
C(ACC)	Minimum Speed	5m/s
	Intended Speed	20 m/s
	Maximum Speed	30 m/s
	Maximum Acceleration	3 m/s^2
	Maximum Deceleration	5 m/s^2
	Platoon Size	5

Fig. 2 presents the speed profile of the platoon members under different circumstances. Fig. 2 (a) shows the platoon member's behavior when no insider adversary is present. When there is no adversary in the platoon, the platoon followers adjust their speed to the leader without any disturbance. In other words, platoon followers follow the leader smoothly where acceleration and deceleration of $Veh1$ are adopted properly. Fig. 2 (b) represents the case where the $Veh1$ is misbehaving and it is insider adversary. $Veh1$ modifies the acceleration field of beacon message such that acceleration is converted to deceleration and vice versa. The altered beacon messages cause speed value fluctuation to platoon followers around that of [0,5] m/s which ruins the platoon stability. On the other hand, Fig. 2 (c) shows the detected anomalies by the platoon followers via the proposed statistical learning based technique. Due to lack of security, vehicles accept the falsified beacon messages from $Veh1$ and use these messages for speed adjustment which leads to platoon instability.

By using statistical learning, almost all the speed anomalies caused by $Veh1$ are successfully detected. However, the proposed algorithm misclassified the speed observations between the times at t = 145 s and t = 172 s. This is due to independent anomaly decision mechanism where vehicles



(a) (b) (c)

Fig. 2: Platoon Member Speed Values (a) No Adversary (b) Leader is Adversary (c) Detected Anomalies

need to cooperate with each other to detect the anomaly in order to decide outlier. After outliers detection, other vehicles can initiate a reliable trust based mechanism where vehicles vote against the misbehaving vehicle to revocate its platoon membership.

V. Conclusion and Future Work

We investigate a data-driven abnormal behavior detection technique and risk associated with the insider misbehaviors in the platoon. We show that due to lack of security, platoon members can be subject to manipulated packets from insider adversary which ruins the platoon stability. With the help of abnormal behavior detection scheme, almost all the speed anomalies are successfully detected.

As future work, we aim to concentrate on designing reliable trust based platoon mechanism that is robust to insider misbehaviors. Such a protocol requires data reception based abnormal behavior detection scheme to explore anomalies in received data, utilizing reputation based system design to collect and model other platoon members feedback and revocating system to remove the rogue vehicles from the platoon membership. Moreover, we also plan to evaluate the performance of reliable trust based platoon mechanism in different metrics associated with misbehaving detection in various scenarios.

References

[1] J. Ploeg, E. Semsar-Kazerooni, G. Lijster, N. van de Wouw, and H. Nijmeijer, "Graceful Degradation of Cooperative Adaptive Cruise Control," *IEEE Transactions on Intelligent Transportation Systems*, vol. 16, no. 1, pp. 488–497, Feb 2015.

[2] J. Lioris, R. Pedarsani, F. Y. Tascikaraoglu, and P. Varaiya, "Platoons of connected vehicles can double throughput in urban roads," *Transportation Research Part C: Emerging Technologies*, vol. 77, pp. 292 – 305, 2017.

[3] S. Santini, A. Salvi, A. S. Valente, A. Pescap, M. Segata, and R. L. Cigno, "A consensus-based approach for platooning with intervehicular communications," in *IEEE Conference on Computer Communications (INFOCOM)*, April 2015.

[4] M. Amoozadeh, H. Deng, C.-N. Chuah, H. M. Zhang, and D. Ghosal, "Platoon management with cooperative adaptive cruise control enabled by VANET," *Vehicular Communications*, 2015.

[5] B. DeBruhl, S. Weerakkody, B. Sinopoli, and P. Tague, "Is Your Commute Driving You Crazy?: A Study of Misbehavior in Vehicular Platoons," in *Proceedings of the 8th ACM Conference on Security & Privacy in Wireless and Mobile Networks*, 2015.

[6] M. Segata, B. Bloessl, S. Joerer, C. Sommer, M. Gerla, R. L. Cigno, and F. Dressler, "Toward Communication Strategies for Platooning: Simulative and Experimental Evaluation," *IEEE Transactions on Vehicular Technology*, Dec 2015.

[7] S. Ucar, S. C. Ergen, and O. Ozkasap, "Security Vulnerabilities of IEEE 802.11p and Visible Light Communication Based Platoon," in *IEEE Vehicular Networking Conference (VNC)*, Dec 2016, pp. 1–4.

[8] F. Qu, Z. Wu, F. Y. Wang, and W. Cho, "A Security and Privacy Review of VANETs," *IEEE Transactions on Intelligent Transportation Systems*, Dec 2015.

[9] H. Hu, R. Lu, Z. Zhang, and J. Shao, "REPLACE: A Reliable Trust-Based Platoon Service Recommendation Scheme in VANET," *IEEE Transactions on Vehicular Technology*, Feb 2017.

[10] J. Zhang, "A Survey on Trust Management for VANETs," in *IEEE International Conference on Advanced Information Networking and Applications*, March 2011.

[11] M. Raya, P. Papadimitratos, V. D. Gligor, and J. P. Hubaux, "On Data-Centric Trust Establishment in Ephemeral Ad Hoc Networks," in *IEEE INFOCOM - The 27th Conference on Computer Communications*, April 2008.

[12] G. Wang and Y. Wu, "BIBRM: A Bayesian Inference Based Road Message Trust Model in Vehicular Ad Hoc Networks," in *IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications*, Sept 2014.

[13] K. Zaidi, M. Milojevic, V. Rakocevic, and M. Rajarajan, "Data-centric Rogue Node Detection in VANETs," in *IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications*, Sept 2014.

[14] A. Wu, J. Ma, and S. Zhang, "RATE: A RSU-Aided Scheme for Data-Centric Trust Establishment in VANETs," in *7th International Conference on Wireless Communications, Networking and Mobile Computing*, Sept 2011.

[15] K. Dixit, P. Pathak, and S. Gupta, "A new technique for trust computation and routing in VANET," in *Symposium on Colossal Data Analysis and Networking (CDAN)*, March 2016.

[16] R. B. Cleveland, W. S. Cleveland, J. E. McRae, and I. Terpenning, "STL: A Seasonal-Trend Decomposition Procedure Based on Loess (with Discussion)," *Journal of Official Statistics*, 1990.

[17] F. R. Hampel, E. M. Ronchetti, P. J. Rousseeuw, and W. A. Stahel, *Robust Statistics: The Approach Based on Influence Functions*, ser. Wiley Series in Probability and Statistics. Wiley, 1986.

[18] F. R. Hampel, *Robust Statistics: The Approach Based on Influence Functions*. University of California, 1986.

[19] B. Rosner, "Percentage Points for a Generalized ESD Many-Outlier Procedure," *Technometrics*, 1983.

[20] M. G. Kendall, A. Stuart, and J. K. Ord, Eds., *Advanced Theory of Statistics*. New York, NY, USA: Oxford University Press, Inc., 1987.

[21] "VEhicular NeTwork Open Simulator (VENTOS)," http://goo.gl/OueFkO.

[22] "R: A language and environment for statistical computing," http://www.R-project.org/.

[23] "Simulation of Urban MObility (SUMO)," http://sumo.sourceforge.net/.

[24] "OMNET++ Networ Simulator," https://omnetpp.org/.

[25] "Vehicles in Network Simulation (Veins)," http://veins.car2x.org/.