Vehicular Platooning to be Secure against Cybersecurity Attacks

Noman Mazher[1], Alsendro Brightini[1], and Farrah Haider[1]

[1]Affiliation not available

July 20, 2022

Abstract

Vehicular platooning is although not a new concept yet reshaping its core idea with invovlment of autonomous driging in it. vehicle platoon is group of vehicle traveling with small space but no physical connection and negligible relative velocity with each other. Platoon can be formed from different type of vehicles such as truck, bus car etc. In platoon each vehicle has a particular role either it is a leader or follower. All of vehicle participating in platoon have to send message to their predecessor vehicle about their present location, and speed velocity. Along with other different challenges such as its trajectory , string stability , maneuvers, platoon communication suffer from security risks. Security is an essential aspects of wireless communication systems Due to the inherent transmission nature of wireless channels.There is a risk of various types of network attacks,Cyberseurity attacks are most common of them. In this research we will reveal the core idea of cybersecurity attacks in autonomous vehicle platooning.

Vehicular Platooning to be Secure against Cybersecurity Attacks

Noman Mazher, Alsendro Brightini, Farrah Haider

Abstract :

Vehicular platooning is although not a new concept yet reshaping its core idea with invovlment of autonomous driging in it. vehicle platoon is group of vehicle traveling with small space but no physical connection and negligible relative velocity with each other. Platoon can be formed from different type of vehicles such as truck, bus car etc. In platoon each vehicle has a particular role either it is a leader or follower. All of vehicle participating in platoon have to send message to their predecessor vehicle about their present location, and speed velocity. Along with other different challenges such as its trajectory , string stability , maneuvers, platoon communication suffer from security risks. Security is an essential aspects of wireless communication systems Due to the inherent transmission nature of wireless channels.There is a risk of various types of network attacks,Cyberseurity attacks are most common of them. In this research we will reveal the core idea of cybersecurity attacks in autonomous vehicle platooning.

Keywords: cybersecurity, vehicular platooning,

I Introduction

Travel demand for humans and freight observed huge increased in number and intensity. This intensity lead increased number of motors not only on urban road but also for long route [1].Along with facilitation, this massive amount of motors bring some problems with this. Major problems are accidents, air pollution and congestion[2]. To decrease carbon footprint and road congestion for improving road safety, The concept of vehicle Platooning proposed[3].By definition vehicle platoon is group of vehicle traveling with small space but no physical connection and negligible relative velocity with each other[4]. Platoon can be formed from different type of vehicles such as truck, bus car etc. In platoon each vehicle has a particular role either it is a leader or follower. All of vehicle participating in platoon have to send message to their predecessor vehicle about their present location, speed velocity etc. This communication can be happen using Vehicle to Vehicle (V2V), Vehicle to Infrastructure (V2I) communication. Famous communication technologies used between vehicles of platoon happen are Dedicated Short Range Communication (DSRC), Long Term Evaluation (LTE) and 5G technologies. Along with other different challenges such as its trajectory , string stability , maneuvers, platoon communication suffer from security risks. Security is an essential aspects of wireless communication systems Due to the inherent transmission nature of wireless channels[5-19].There is a risk of various types of network attacks such as DOS , Man in Middle, Masquerading attacks, Impersonation, Eves Dropping, Jamming, Location Spoofing, Location tracking, Sybil attacks etc[20, 21]. These attacks can be happened from both outside vehicles and also from platoon members

Conclusion:

Vehicular platooning is although not a new concept yet reshaping its core idea with invovlment of autonomous driging in it. vehicle platoon is group of vehicle traveling with small space but no physical connection and negligible relative velocity with each other. Platoon can be formed from different type of vehicles such as truck, bus car etc. In platoon each vehicle has a particular role either it is a leader or follower. All of vehicle participating in platoon have to send message to their predecessor vehicle about their present location, and speed velocity. Along with other different challenges such as its trajectory , string stability , maneuvers, platoon communication suffer from security risks. Security is an essential aspects of wireless communication systems Due to the inherent transmission nature of wireless channels.There is a risk of various types of network attacks,Cyberseurity attacks are most common of them. In this research we will reveal the core idea of cybersecurity attacks in autonomous vehicle platooning.

Refrences:

[1] A. Alnasser and H. Sun, "Global roaming trust-based model for V2X communications," in *IEEE INFOCOM 2019-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, 2019: IEEE, pp. 1-6.

[2] A. Ghosal *et al.*, "Truck platoon security: State-of-the-art and road ahead," *Computer Networks,* vol. 185, p. 107658, 2021.

[3] L. Yang, Z. Liu, Y. Zeng, S. Mei, and J. Ma, "Security Mechanisms to Provide Convoy Member Co-presence Authentication in Vehicle Platooning," in *2019 International Conference on Networking and Network Applications (NaNA)*, 2019: IEEE, pp. 58-63.

[4] F. Boeira, M. P. Barcellos, E. P. de Freitas, A. Vinel, and M. Asplund, "Effects of colluding Sybil nodes in message falsification attacks for vehicular platooning," in *2017 IEEE Vehicular Networking Conference (VNC)*, 2017: IEEE, pp. 53-60.

[5] M. Du, Z. Chen, C. Liu, R. Oak, and D. Song, "Lifelong anomaly detection through unlearning," in *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, 2019, pp. 1283-1297.

[6] H. Jain, R. Oak, and J. Bansal, "Towards Developing a Secure and Robust Solution for E-Voting using Blockchain," in *2019 International Conference on Nascent Technologies in Engineering (ICNTE)*, 2019: IEEE, pp. 1-6.

[7] K. S. Jhala, R. Oak, and M. Khare, "Smart collaboration mechanism using blockchain technology," in *2018 5th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2018 4th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom)*, 2018: IEEE, pp. 117-121.

[8] M. Khare and R. Oak, "Real-Time distributed denial-of-service (DDoS) attack detection using decision trees for server performance maintenance," in *Performance Management of Integrated Systems and its Applications in Software Engineering*: Springer, 2020, pp. 1-9.

[9] J. C. Newman and R. Oak, "Artificial Intelligence: Ethics in Practice," *login Usenix Mag.,* vol. 45, no. 1, 2020.

[10] R. Oak, "A study of digital image segmentation techniques," *Int. J. Eng. Comput. Sci,* vol. 5, no. 12, pp. 19779-19783, 2016.

[11] R. Oak, "Extractive techniques for automatic document summarization: a survey," *International Journal of Innovative Research in Computer and Communication Engineering,* vol. 4, no. 3, pp. 4158-4164, 2016.

[12] R. Oak and M. Khare, "A novel architecture for continuous authentication using behavioural biometrics," in *2017 International Conference on Current Trends in Computer, Electrical, Electronics and Communication (CTCEEC)*, 2017: IEEE, pp. 767-771.

[13] R. Oak, "A literature survey on authentication using Behavioural biometric techniques," *Intelligent Computing and Information and Communication,* pp. 173-181, 2018.

[14] R. Oak, M. Khare, A. Gogate, and G. Vipra, "Dynamic Forms UI: Flexible and Portable Tool for easy UI Design," in *2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT)*, 2018: IEEE, pp. 1926-1931.

[15] R. Oak, M. Du, D. Yan, H. Takawale, and I. Amit, "Malware detection on highly imbalanced data through sequence modeling," in *Proceedings of the 12th ACM Workshop on artificial intelligence and security*, 2019, pp. 37-48.

[16] R. Oak, "Poster: Adversarial Examples for Hate Speech Classifiers," in *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, 2019, pp. 2621-2623.

[17] R. Oak, C. Rahalkar, and D. Gujar, "Poster: Using generative adversarial networks for secure pseudorandom number generation," in *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, 2019, pp. 2597-2599.

[18] R. Oak, "The Fault in the Stars: Understanding the Underground Market of Amazon Reviews," *arXiv preprint arXiv:2102.04217,* 2021.

[19] V. Sehwag, R. Oak, M. Chiang, and P. Mittal, "Time for a background check! uncovering the impact of background features on deep neural networks," *arXiv preprint arXiv:2006.14077,* 2020.

[20] M. Muhammad and G. A. Safdar, "Survey on existing authentication issues for cellular-assisted V2X communication," *Vehicular Communications,* vol. 12, pp. 50-65, 2018.

[21] A. Masood, D. S. Lakew, and S. Cho, "Security and Privacy Challenges in Connected Vehicular Cloud Computing," *IEEE Communications Surveys & Tutorials,* vol. 22, no. 4, pp. 2725-2764, 2020.