# Cybersecurity Attacks in Celluler-V2X Communicaiton Networks

Noman Mazher, Mohmmad Alhaddad, Oyunchimeg Shagdar

## Abstract:

Vehicles in the current era can communicate with other vehicles, roadside units, and networks. This communication is collaboratively called Vehicle to Everything(V2X) communication. V2X network leverages modern communication technologies such as DSRC, LTE, and 5G communication. Along with the leverages of these technologies, potential security threat has also increased. Cybersecurity attacks are the most common attacks that damage the V2X communication network. In this paper, we will reveal poetnetial cybersecurity attacks in V2X communication

Keywords: V2X communication, cybersecurity attacks, V2X security

## Introduction:

The growth of the human population brings numerous challenges; transportation is one of its challenges. As much as the human population increases, more transport facilities are required. The number of roadside vehicles increased proportionally with the human population. This massive number of vehicles on the road brings new challenges such as traffic jams, roadside accidents resulting in loss of precious human life, polluted atmosphere, noise pollution, and many more. Vehicles in the current era can communicate with other vehicles, roadside units, and networks. This communication is called Vehicle to Everything(V2X) communication. . V2X network leverages modern communication technologies such as DSRC, LTE, and 5G communication.

Along with the leverages of these technologies, potential security threat has also increased. Cybersecurity attacks are the most common attacks that damage the V2X communication network. In this paper, we will reveal potential cybersecurity attacks in V2X communication.

Security is an intergeral part of each technologiy and simultaneously increases its demand as much as technology increases[1-5]. Figure 1 is presenting an overview of V2X communication network. V2X communication network mainly formed by vehicle to vehicle communication(V2V), Vehicle to Network communication (V2N), Vehicle to Pedestarian communication (V2P) and Vehicle to Infrastruture communication (V2I).

Cybersecurity is one of the major security issue in todays technology gloab[6-20]. In this paper we will reveal cybersecurity threats in V2X communication netwok.

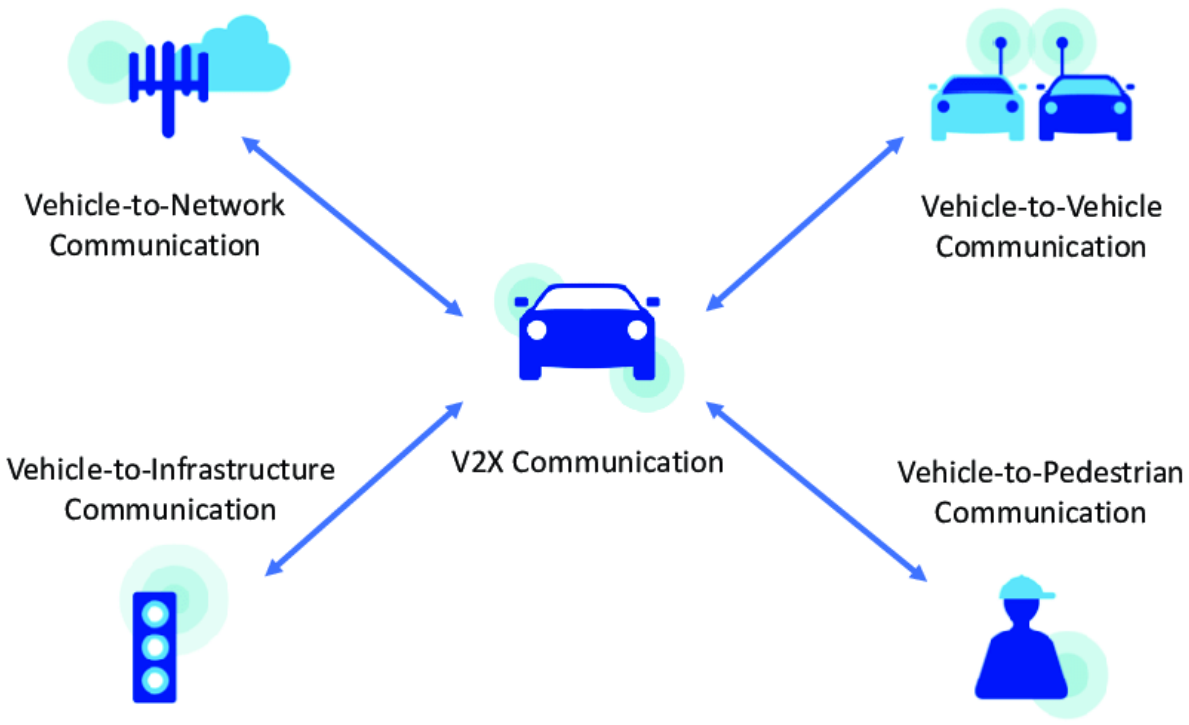


Fig 1: overview of V2X communication network

## Cybersecurity attacks in V2X communication:

In this section we will give an overview of cybersecurity threats commonly found from our literature rev iew in V2X communication network.

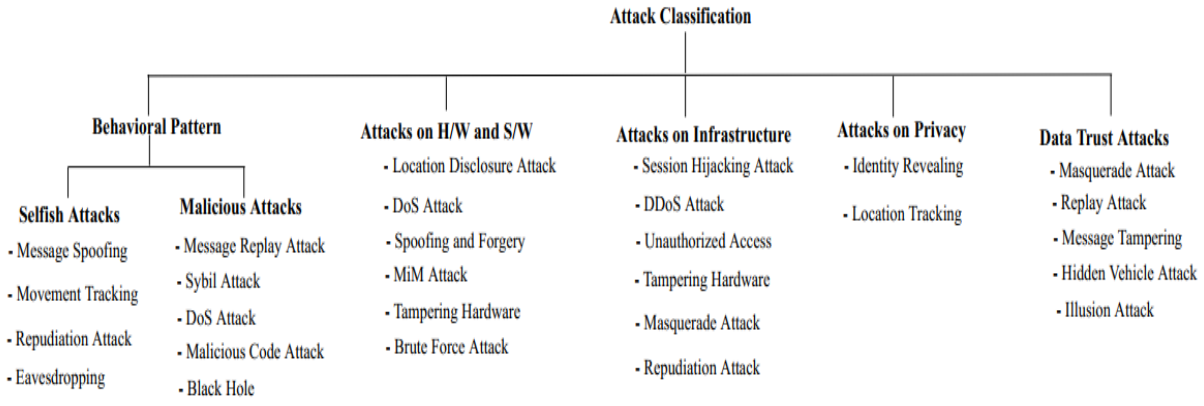


Fig 2: Attack classification in V2X communication security

## Conclusion

In this research we conducted a survey on cybersecurity attacks on vehicle to everything network. Cybersecurity is most common security threat in all kind of network. V2X communication network also suffer from cybersecurity attack. Since the daynamic nature of V2X need more intension on inherited security issues of cybersecurity attacks, and demand extra security features for cybersecurity attacks. Our research can play a vital role for new researcher in V2X communication security researchers.

**Refremces:**


[1] M. Ahmadi and B. S. Ghahfarokhi, "Preserving privacy in location based mobile coupon systems using anonymous authentication scheme," in *2016 13th International Iranian Society of Cryptology Conference on Information Security and Cryptology (ISCISC)*, 2016: IEEE, pp. 60-65.

[2] M. Ahmadi, "Hidden fear: Evaluating the effectiveness of messages on social media," Arizona State University, 2020.

[3] M. Ahmadi, K. Leach, R. Dougherty, S. Forrest, and W. Weimer, "Mimosa: Reducing malware analysis overhead with coverings," *arXiv preprint arXiv:2101.07328,* 2021.

[4] M. Ahmadi, P. Kiaei, and N. Emamdoost, "SN4KE: Practical Mutation Testing at Binary Level," *arXiv preprint arXiv:2102.05709,* 2021.

[5] P. Kiaei, C.-B. Breunesse, M. Ahmadi, P. Schaumont, and J. Van Woudenberg, "Rewrite to reinforce: Rewriting the binary to apply countermeasures against fault injection," in *2021 58th ACM/IEEE Design Automation Conference (DAC)*, 2021: IEEE, pp. 319-324.

[6] 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.

[7] 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.

[8] 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.

[9] 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.

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

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

[12] 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.

[13] 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.

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

[15] 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.

[16] 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.

[17] 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.

[18] 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.

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

[20] 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.