Cybersecurity Of Autonomous Vehicle Platooning

Presenter: Soodeh Dadras
Advisor: Prof. Chris Winstead
Electrical and Computer Engineering Department
Utah State University

Agenda

- What is Autonomous Vehicle Platooning?
- Pros and Cons of Autonomous Vehicle Platooning
- Platooning Challenges
- Modeling and Results
- Conclusion

Autonomous Vehicle Platooning

- **Autonomous Vehicle:**
  - The car that drives itself.

- **Platooning:**
  - Group of Autonomous vehicles travelling together with relatively small spacing and small/zero relative velocity of the vehicles.

Leading Companies and Projects

Pros and Cons

- **Pros:**

1. Safety
2. Operational Efficiency (Increase highway capacity)
3. Driving Comfort
4. Transit time Efficiency

- **Cons:**

1. Computer failure
2. Degrading performance in case of interception
3. Increase in crashes involving pedestrians

Platooning Challenges

- Driver acceptance
- Reliability
- Legislation
- System Security

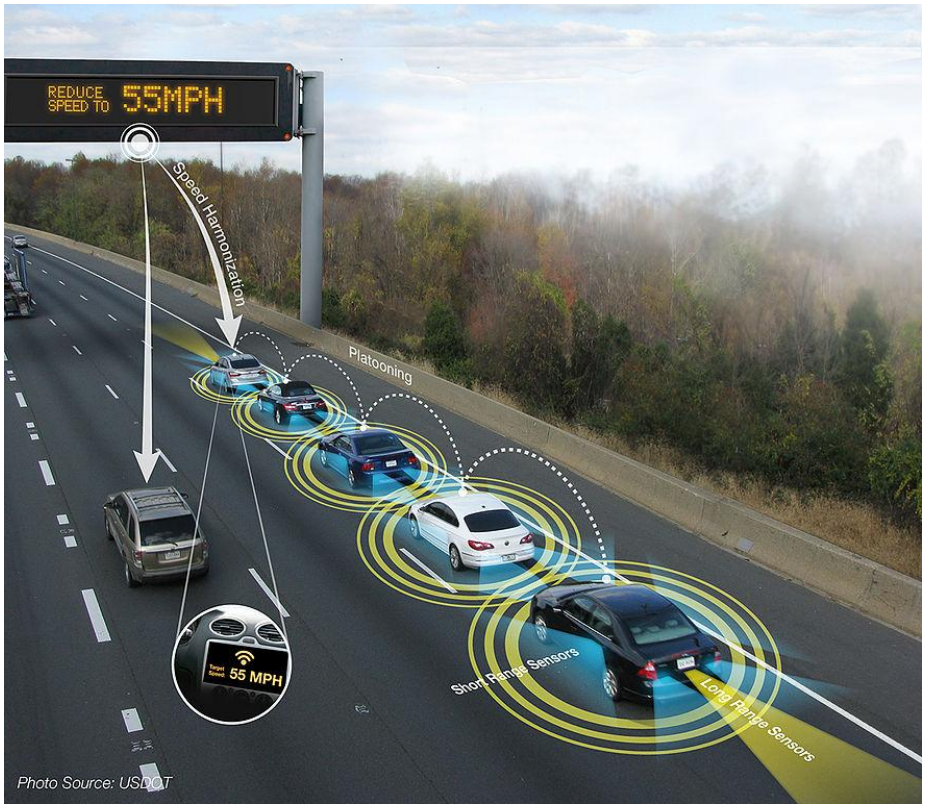
Cyber Security Of Autonomous Vehicle Platooning

"In fact, Munich Re, the world's second-largest reinsurer, found that **55 %** of corporate risk managers surveyed in a recent study named **cybersecurity** as their **top concern** for autonomous vehicles. Even more alarming, **64 %** of companies surveyed say they feel completely **unprepared** to address cyber security [1] "

Research Works Study the Security in Platooning

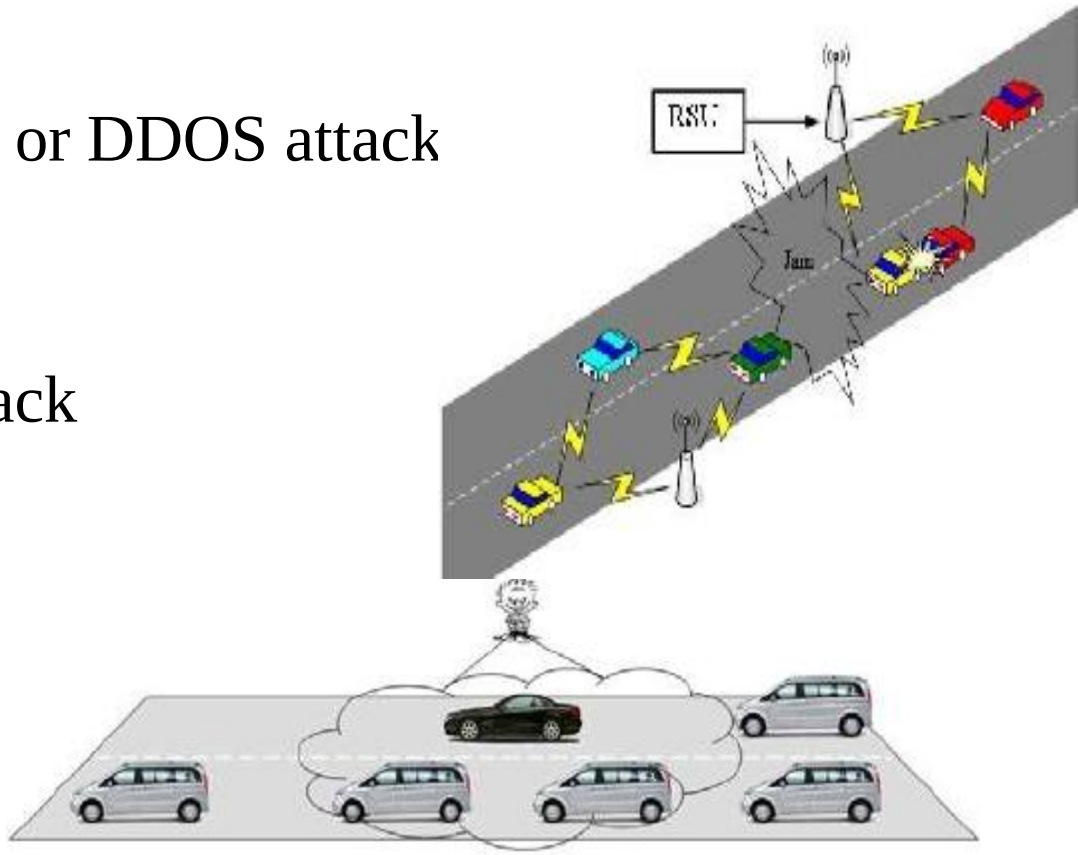
- **Communication security issues** [2,3]

  - Availability
  - Confidentiality
  - Data integrity
  - Authentication



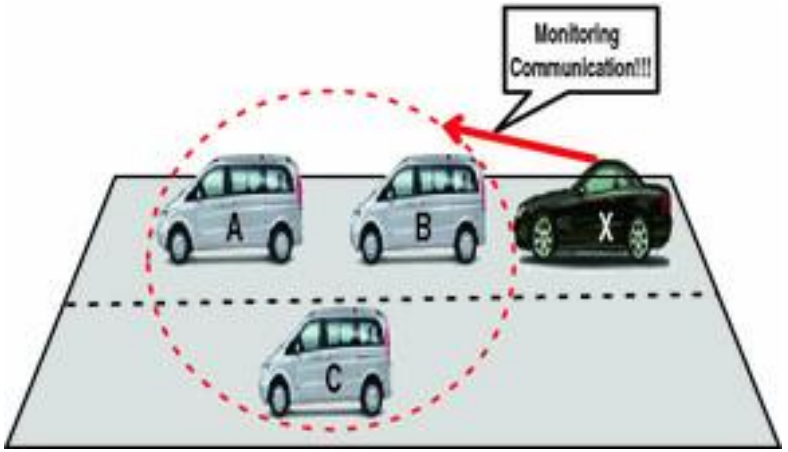
Security Attacks on Communication: Threats and Attacks on Availability

- Jamming attack
- DOS (Denial of service) or DDOS attack
- Malware attack
- Broadcast tampering attack
- Black hole attack
- Greedy behavior attack
- Spamming attack



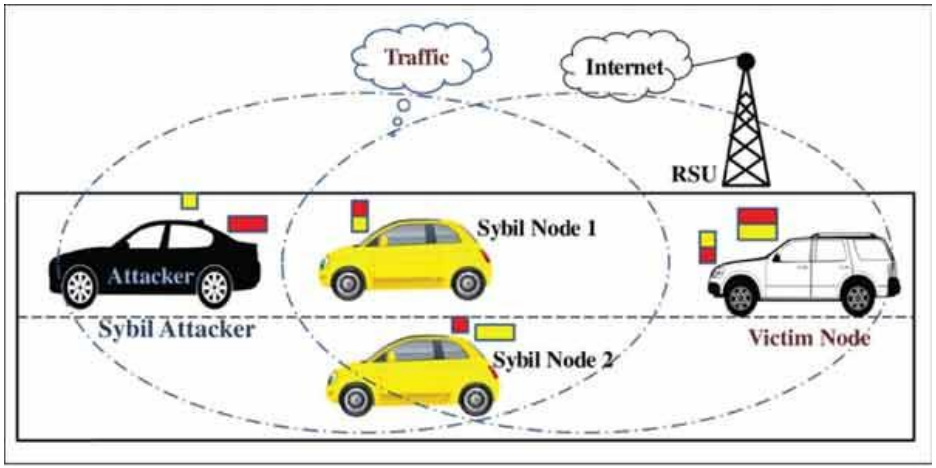
Security Attacks on Communication: Threats and Attacks on Confidentiality

- Eavesdropping attack
- Traffic analysis attack
- Man in the middle attack



Security Attacks on Communication: Threats and Attacks on Authentication

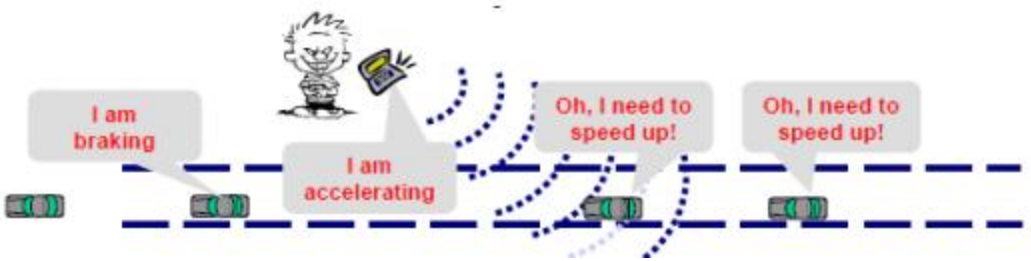
- Sybil attack
- Tunneling attack
- GPS spoofing
- Impersonation attack



- Free-riding attack (or active free-riding attack)
- Masquerading attack
- Key and/or certificate replication
- Message tampering

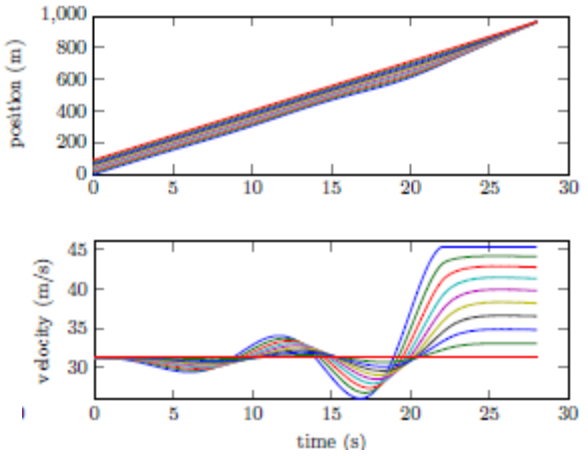
Security Attacks on Communication: Threats and Attacks on Data Integrity

- Replay attack
- Masquerading attack
- Message modification attack
- Illusion attack



Research Works Study Security In Platooning

- **Control security issues**

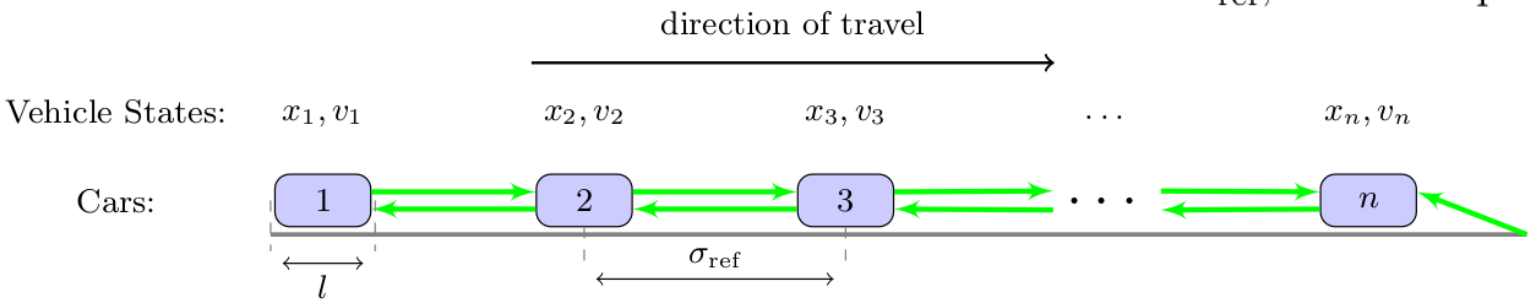


- Destabilizing attack [4]
- High-speed Collision induction attack [5]
- Energy efficiency attack [6]
- False data injection [7]
- Traffic flow instability attack [8]

Platoon Model

- Bidirectional structure [9]:

x_i, car i's position
v_i, car i's velocity
l, car length
σ_{ref}, desired separation

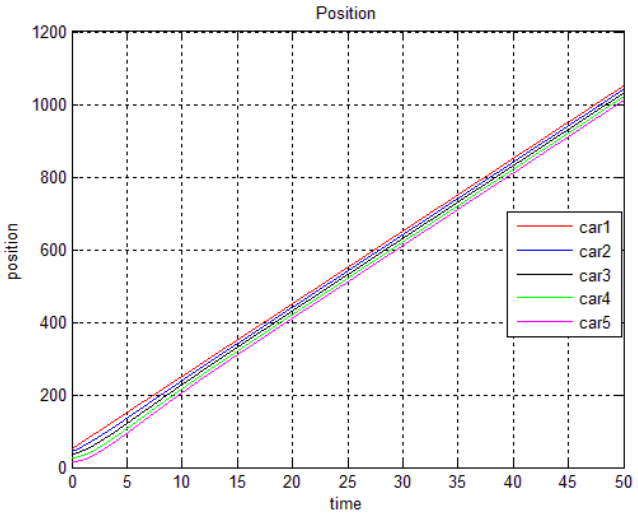


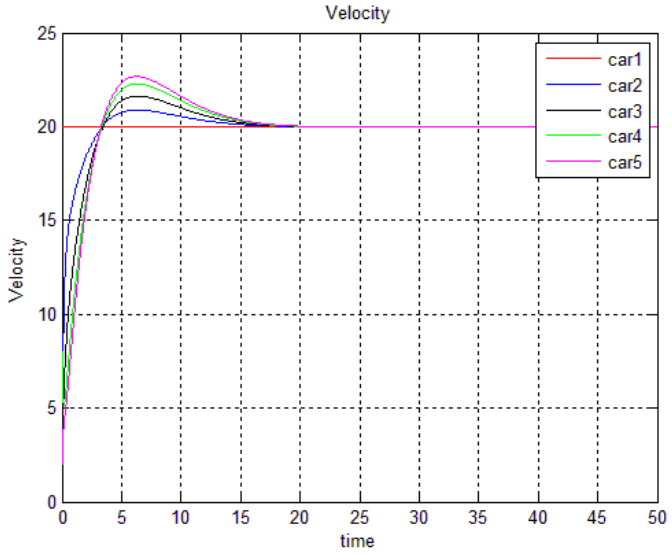
Each vehicle receives states of the vehicles in front and behind.

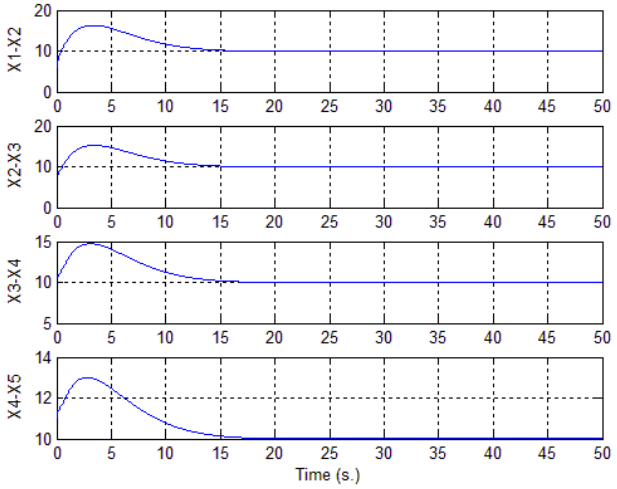
$$u_i = k_p(x_{i+1} - x_i - \sigma_{\text{ref}}) + k_p(x_{i-1} - x_i + \sigma_{\text{ref}}) + k_d(v_{i+1} - v_i) + k_d(v_{i-1} - v_i)$$

with k_p position gain and,
with k_d velocity gain

System Performance







Attack Model

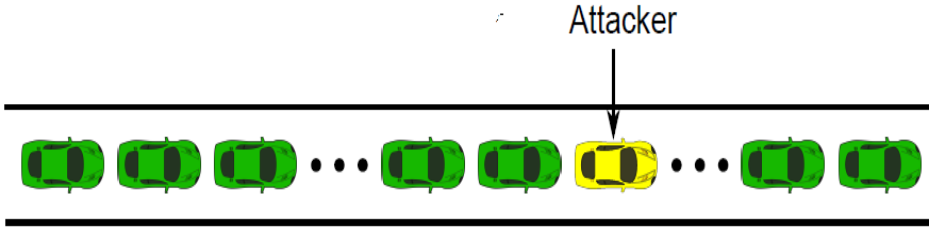
- Attack objective

  Causing **collision** by attackers' motion and gain modification

While:

Attacker is not affected

Attacker is not detectable



$$u_i = k_p(x_{i+1} - x_i - \sigma_{ref}) + k_p(x_{i-1} - x_i + \sigma_{ref}) + k_{d_a}(v_{i+1} - v_i) + k_{d_a}(v_{i-1} - v_i) + \mathrm{u}_a$$

k_{d_a} : *velocity gain for the attacker*

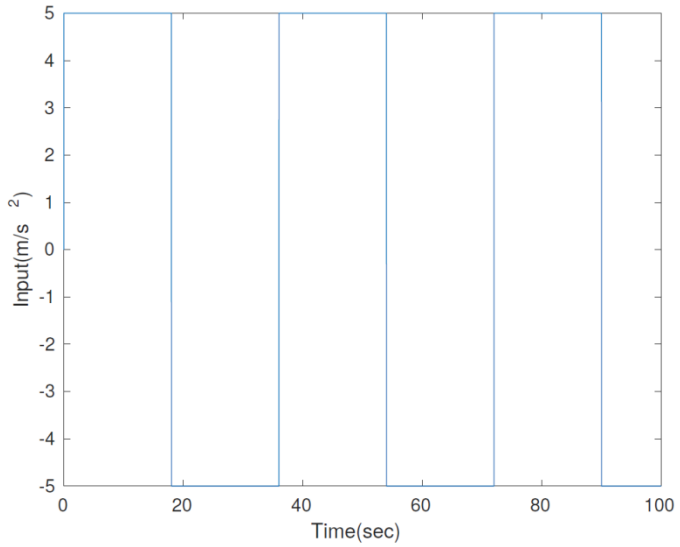
u_a : *Attacker's input*

Simulation Results

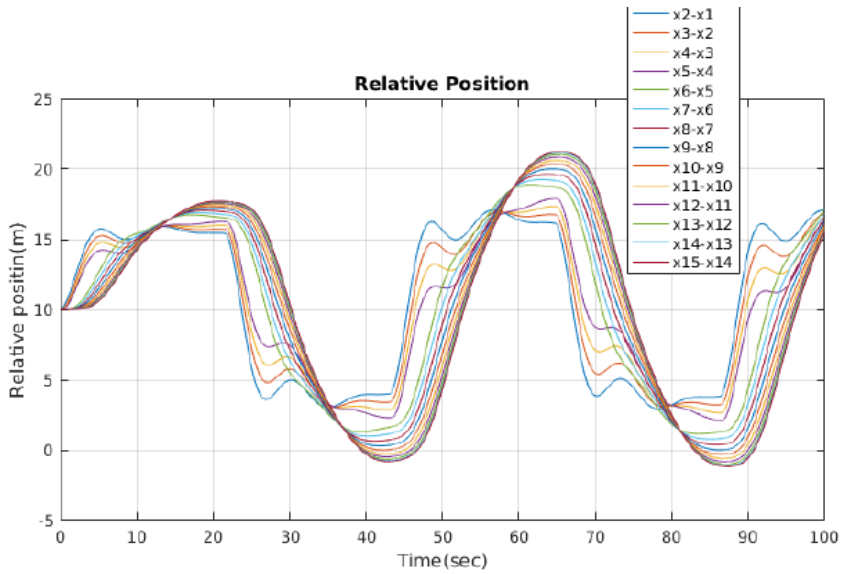
- 15-vehicle platoon
- Attackers # 1 and #5
- Gains for normal and attacker's vehicle
- Attacker’s Input

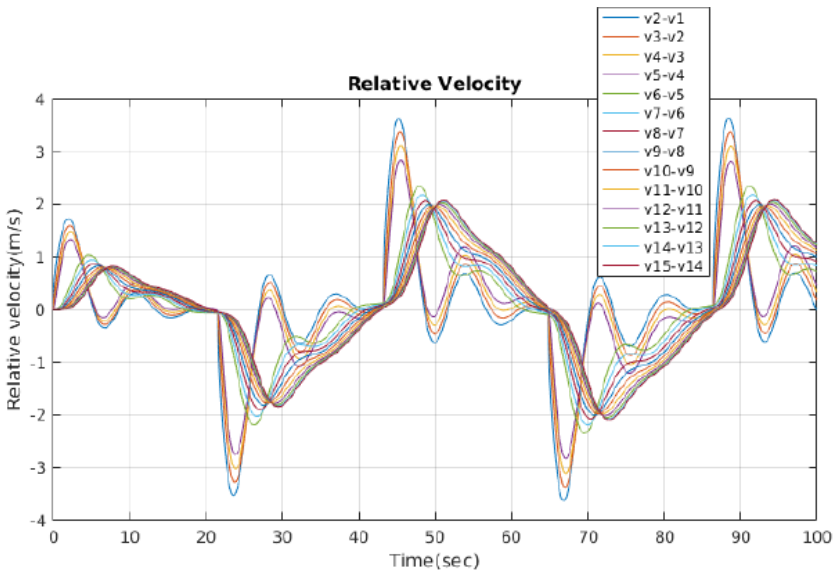
$$k_p = 1, k_d = 11$$

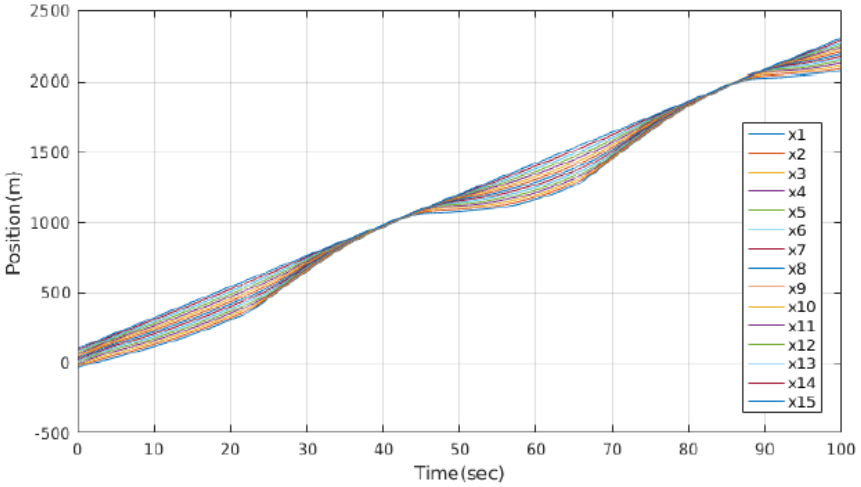
$$k_{d_a} = 0.3$$

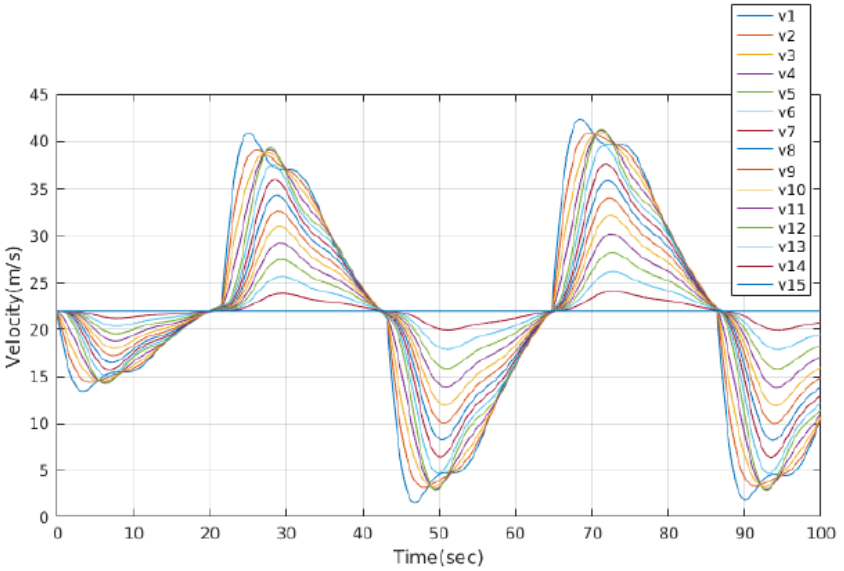


Simulation Results

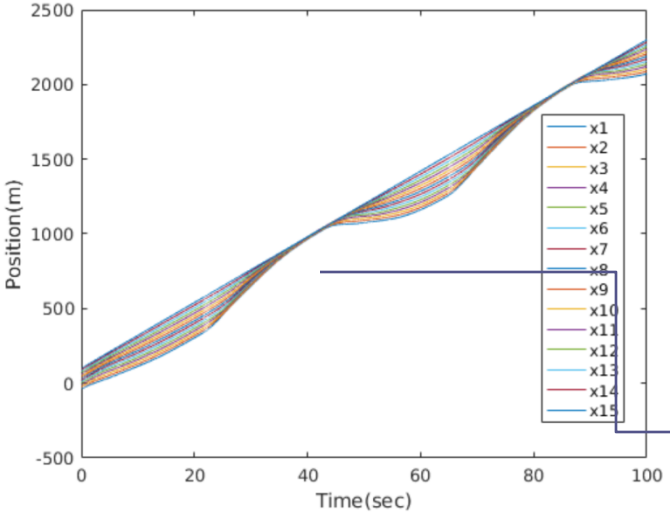


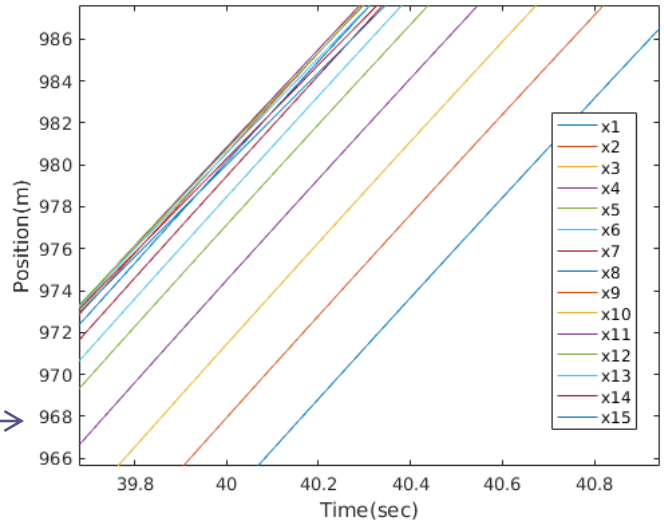


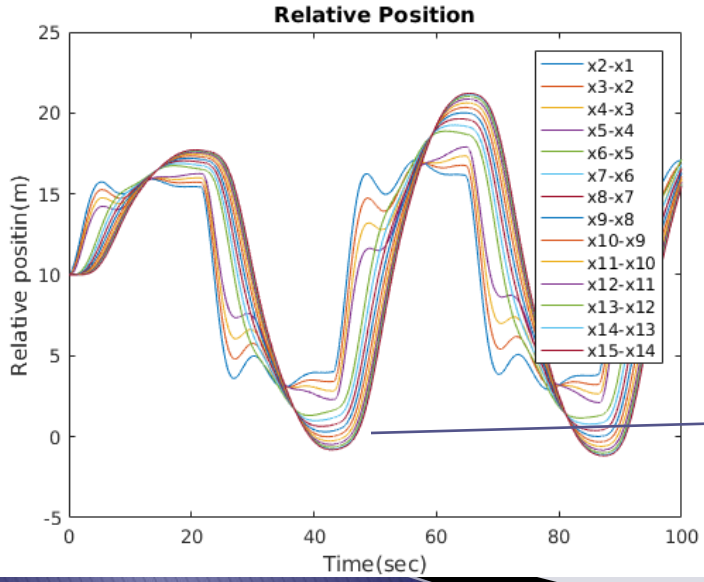


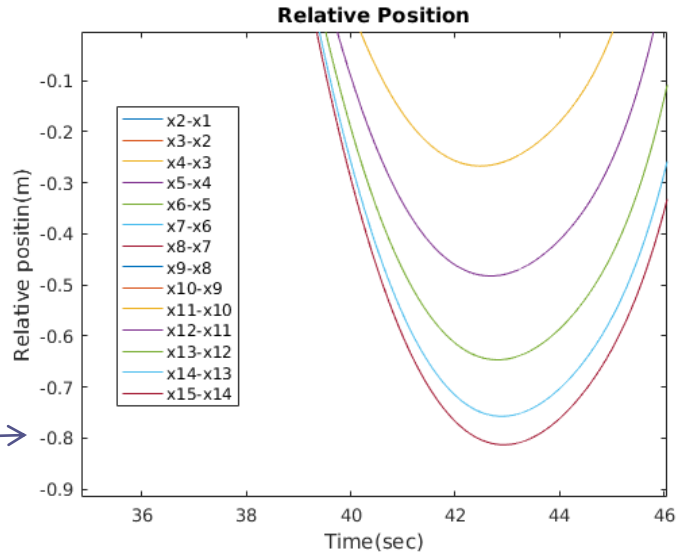


Simulation Results









Conclusion

- Simulation results show:

  - Attacker can easily disrupt platoon performance and stay **intact** and Attacker is **not detectable**.

  - Cyber security of autonomous vehicle platooning is an important issue and it needs immediate attention.

Bibliography

[1] https://techcrunch.com/2017/02/18/why-a-cybersecurity-solution-for-driverless-cars-may-be-found-under-the-hood

[2] Amoozadeh, M., Raghuramu, A., Chuah, C. N., Ghosal, D., Zhang, H. M., Rowe, J., & Levitt, K. (2015). Security vulnerabilities of connected vehicle streams and their impact on cooperative driving. *IEEE Communications Magazine*, *53*(6), 126-132.

[3] Azees, M., Vijayakumar, P., & Deborah, L. J. (2016). Comprehensive survey on security services in vehicular ad-hoc networks. *IET Intelligent Transport Systems*, *10*(6), 379-388.

[4] Dadras, S., Gerdes, R. M., & Sharma, R. (2015, April). Vehicular platooning in an adversarial environment. In *Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security* (pp. 167-178). ACM.

[5] DeBruhl, B., Weerakkody, S., Sinopoli, B., & Tague, P. (2015, June). 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* (p. 22). ACM.

[6] Gerdes, R. M., Winstead, C., & Heaslip, K. (2013, December). CPS: an efficiency-motivated attack against autonomous vehicular transportation. In *Proceedings of the 29th Annual Computer Security Applications Conference* (pp. 99-108). ACM.

[7] Biswas, B. (2015). *Analysis of false data injection in vehicle platooning*. Utah State University.

[8] Dunn, D. D. (2015). *Attacker-induced traffic flow instability in a stream of automated vehicles*. Utah State University.

[9] Yanakiev, D., & Kanellakopoulos, I. (1996, July). A simplified framework for string stability analysis in AHS. In *Proceedings of the 13th IFAC World Congress* (Vol. 182, pp. 177-182).