NSF REU SIte on Secure, Accessible, and Sustainable Transportation: Summer 2025

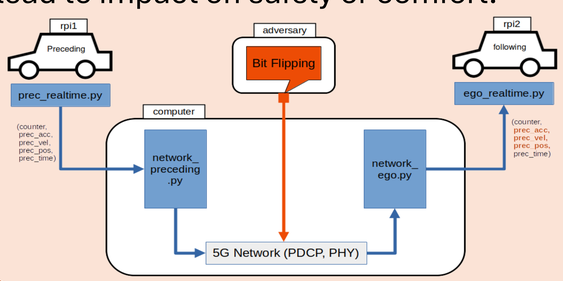
# Impact Analysis of Network-Level Bit-Flipping Attacks on Cooperative Adaptive Cruise Control in 5G Environment

Joon Kim, Chengwei Duan, Sandip Ray

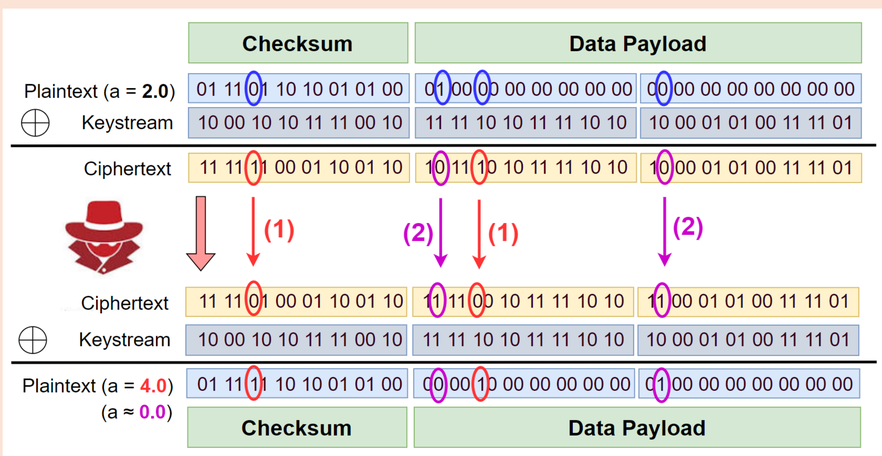
## Abstract

Identified a threat model in 5G without integrity protection to develop a Man-in-the-Middle bit-flipping on floats.

Some attacks on specific bit positions lead to impact on safety or comfort.




## Bit Flipping Attack




In 5G CACC applications, integrity protection is often disabled to prevent DoS. Then, we can define two modes of bit-flipping attacks:

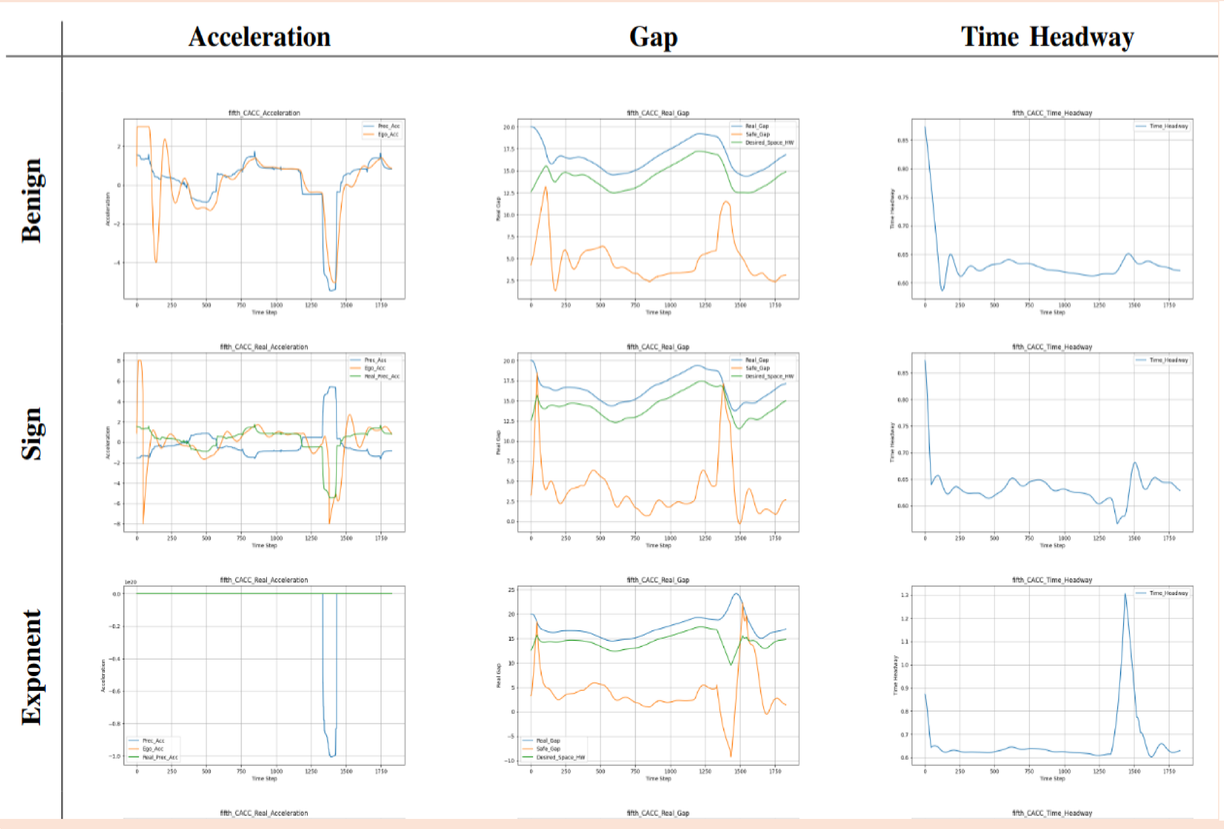
(1) Single-channel attacks that flips one bit of the acceleration value and an aligning checksum bit, success rate 50%.
(2) Multi-channel attacks that can flip up to two bits that are aligned and is not guaranteed 50% success rate.

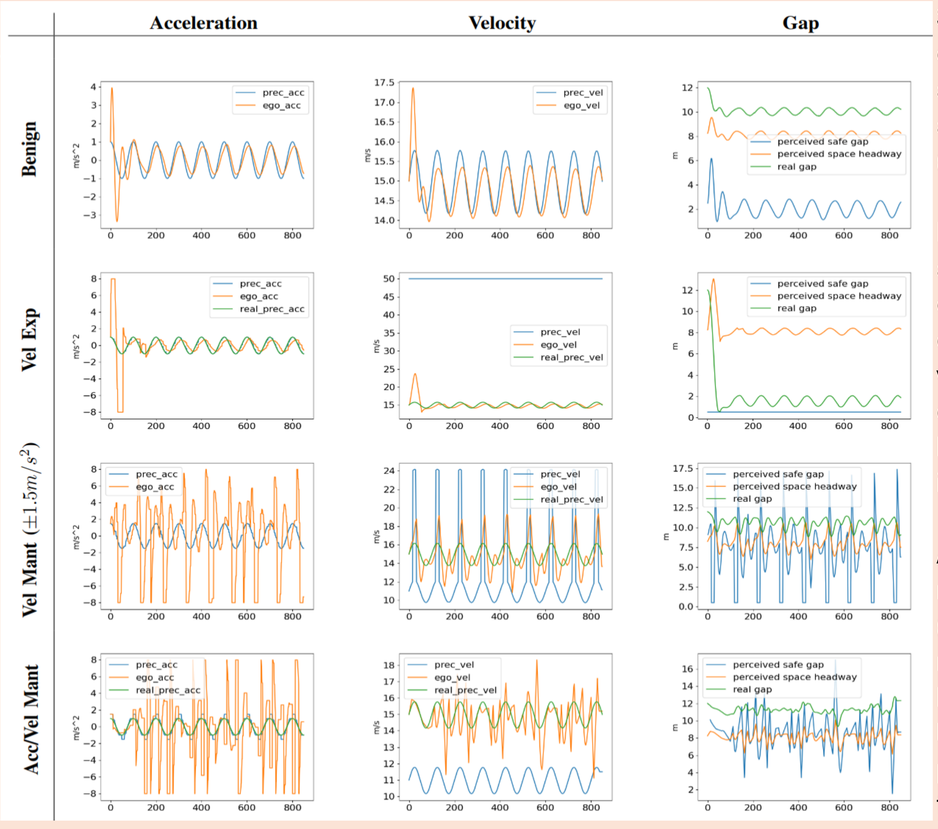
## Conclusion and Future Work

While only successful 50% of the time in expectation and able to flip at most two bits, multi-channel attacks can impact safety and comfort in 5G CACC applications.

Future work include designing scalable and DoS-resilient defense with Error Correcting Codes and investigating impacts of bit-flipping on CAV scenarios modeled by multi-channel.

## Results




Single-channel attack is only impactful when the absolute value of acceleration value is large (exponent).

In multi-channel attacks, attacking only the exponent of the velocity caused the following vehicle to drive extremely close to the preceding vehicle, causing safety issues.

Also, attacking the mantissa of the velocity (or with acceleration mantissa) causes jerky behavior in acceleration, leading to discomfort of passengers in the following vehicle.