講演番号	262

The Application of Encrypted Control Technology to CACC

Takaharu Yamada [1)] **Kiminao Kogiso** [2)]

1) dSPACE Japan K.K.
10F Gotenyama Trust Tower, 4-7-35 Kita-shinagawa, Shinagawa-ku, 140-0001 Tolyo, Japan
2) The University of Electro-Communications
1-5-1 Chofugaoka, Chofu, Tokyo 182-8585, Japan

KEY WORDS: **Information, Communication, and Intelligence, Secure communication protocol, inter-vehicle communication/vehicle-to vehicle communication**, Encrypted control [E2]

In recent years, as wireless communication has become increasingly prevalent in the automotive field, cooperative cruise control (CACC) using vehicle-to-vehicle(V2V) communication has attracted growing attention. CACC enables platoon driving while maintaining inter-vehicle distance, thereby reducing driver burden and alleviating traffic congestion. However, wireless communication is inherently vulnerable to eavesdropping and interference. In this study, we apply encrypted control to CACC, referred to as *Encrypted-Control-Based CACC*, and demonstrate that the desired inter-vehicle distance can be maintained. Furthermore, through hardware implementation and simulation, we verify that tampering with communication data can be detected due to the inherent characteristics of encrypted control.

Regarding Fig. 1, in the leader vehicle's ECU, the data to be transmitted, denoted as α_{i-1}, v_{i-1}, $Dist_{i-1}$, and L_{Dist} are encrypted. Similarly, the follower vehicle's ECU and sensors encrypt their speed v_i and distance $Dist_i$ before transmission. The follower ECU performs secure computations using the received ciphertexts together with encrypted control parameters $C_{K0,[n]}$, $C_{K1,[n]}$, and $C_{K2,[n]}$, generating the ciphertext $C_{u[i]}$ corresponding to the control input through ciphertext multiplication based on the properties of the ElGamal cryptosystem. Decryption is carried out in the vehicle's Brake/Accel module, where addition and subtraction are performed after decryption to obtain the final control input u_i.

Fig. 2 shows the results of Encrypted-Control-Based CACC when the target inter-vehicle distance is set to 10 m. In the simulation, the follower vehicle maintains a 10 m gap while following the leader vehicle along the WLTC class 3b speed profile using Encrypted-Control-Based CACC. Throughout the 1800s simulation, the inter-vehicle distance remains within ±1.0 m of the target, confirming the effectiveness of the proposed implementation.

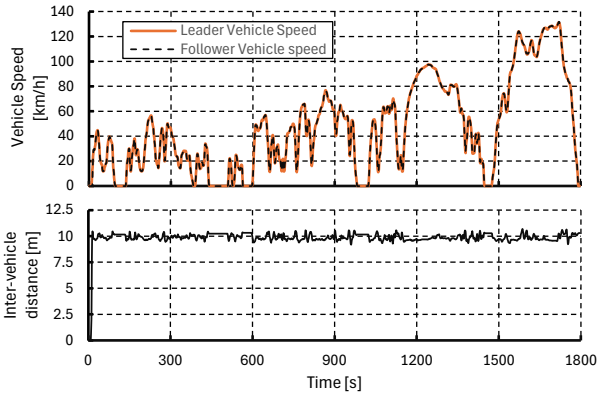

Fig. 2 Result of WLTC class 3b with Encrypted-Control-Based CACC

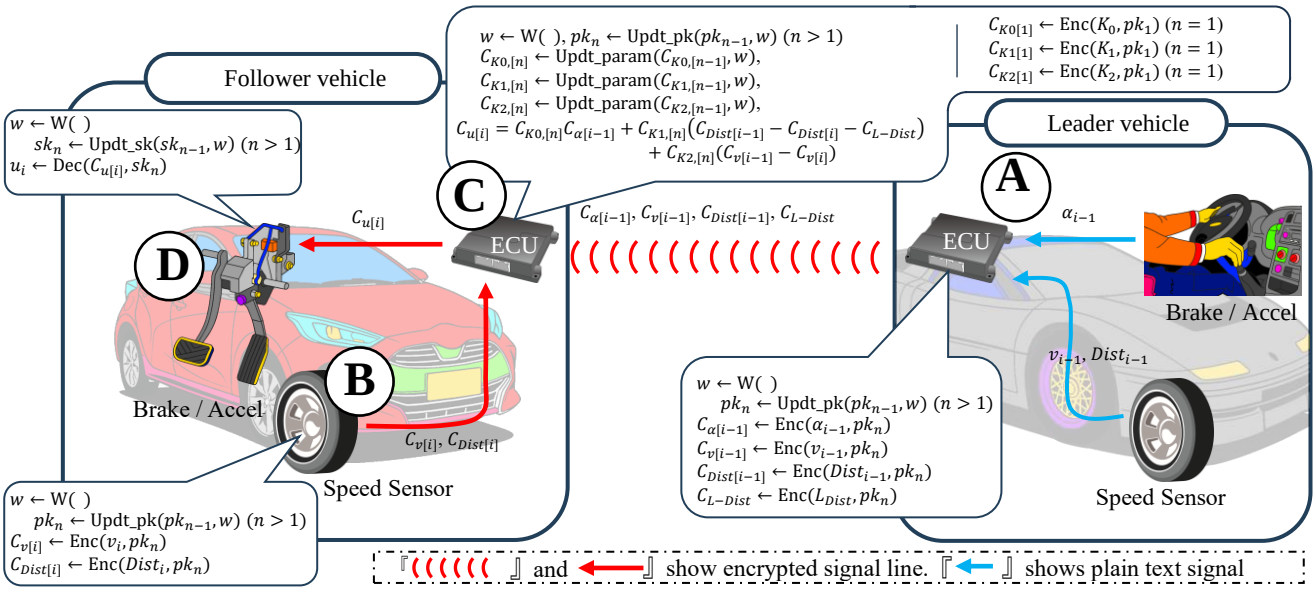

Fig. 1 Encrypted-Control-Based CACC