Analyzing the Impact of Secure CAN Networks on Braking Dynamics of Cooperative Driving

Dharshan Krishna Murthy, Mingqing Zhang, and Alejandro Masrur
Department of Computer Science
TU Chemnitz, Germany

***Abstract*—With the advent of cooperative driving, vehicles can travel at very short distances between them. These vehicle arrangements lead to fuel savings due to the reduced aerodynamic forces. However, the braking situations can be extremely dangerous due to the short vehicle distances. Therefore, a solution has to be devised for safe and collision-free braking. Additionally, such vehicle arrangements have to also be protected from cyber attacks so that no intruder can take over vehicle control. The in-vehicle sensors together with secure in-vehicle networks can be efficiently used for both braking and at the same time shielding the vehicle from intruders with malicious intent.**

***Index Terms*—Cooperative Intelligent Transport Systems (ITS), platoons, braking, cybersecurity, CAN networks, AES, OCB, authentication, encryption**

I. Introduction

Applications like convoys/platoons, part of the Cooperative Intelligent Transport Systems (ITS) are gaining importance and are seen as a step change towards autonomous driving. In such vehicle arrangements, the inter-vehicle separations are between 5 to 10 meters [1]. These short separations leads to improved traffic flow and driver comfort as the vehicle maneuvers are performed by control systems [1] [2] [3]. Additionally, due to the reduced aerodynamic forces on the following vehicles, fuel/energy savings result. In fact, wind tunnel experiments have demonstrated optimum fuel/energy savings for the whole convoy, including the lead, when the separations are just about 1 meter [4] [5].

To facilitate safe convoy operation at separations of just 1 meter, critical information like the lead vehicle's speed, position, and acceleration/deceleration have to be communicated to all vehicles within the shortest possible delay. This is particularly more important in braking than cruise situations. If this requirement is not met, collisions may happen, endangering the lives of in-vehicle passengers and of other road users.

The critical information can be broadcasted wirelessly as per the IEEE 802.11p standard [6] adapted in Europe by the European Telecommunications Standards Institute (ETSI) [7]. However, due to random access nature of the Medium Access Control (MAC) [8], packet losses and distortions impose limitations on the achievable delay.

Another important factor is the security aspect of these wireless communications. The adhoc vehicle network has to be shielded from external intruders with malicious intents. There have been several instances where intruders have hacked into in-vehicle networks and taken over control of the vehicle [9] [10]. The Electronic Control Units (ECU) that rely on the Internet Protocol (IP) for providing certain services, and the ones that wirelessly exchange information are typical targets of such attacks.

Therefore, for implementing cooperative driving with separations of just 1 meter, suitable solutions have to be devised. Particularly, during braking, the following vehicles have to initiate the necessary maneuvers within the shortest delay possible. Further, the solution has to also be secure from external cyberattacks.

Contributions: In this paper, we demonstrate safe collision-free braking in cooperative driving at separations of 1 meter. We assume that an in-vehicle short-range radar is used and secure the CAN network communication to the brake controller and brake actuators using authenticated encryption. Due to relying on in-vehicle sensors, data can be sampled at a faster rate. However, the security overhead on the bus impacts the achievable message transmission delay. Since related messages cannot always be assigned the highest priorities, due to other hard real time systems sharing the bus, we propose a dynamic encryption switching scheme that aims at minimizing encryption overhead and, hence, also delays related to it.

II. Related Work

The benefits of cooperative driving were first demonstrated by the PATH program [4] [5]. More recently, systems to enable vehicles to participate in cooperative driving were developed in the SARTRE project [1]. Apart from these, controllers based on classical design techniques have been proposed for the cruise situation [11] [12] [13]. These controllers ensure that *string stability* [14] is guaranteed.

Emergency braking in cooperative driving was considered in [15]. The shortest vehicle separation considered in this work was 2 meters. However, this approach does not consider security, even though it relies on wireless messages for inter-vehicle communications. We differ from the mentioned approach by relying on in-vehicle sensors and secure network communications. Further, our vehicle separations are only 1 meter. In [16], the maximum tolerable wireless communication delay to avoid the following vehicle crashing into its immediate lead was studied.

From the perspective of CAN network security, new protocols like LiBrA-CAN [17] and MacCAN [18] have been developed. However, the associated higher costs, and the need

to modify the CAN protocol entirely, limits their implementation. As an alternative to changing the CAN protocol, [19] uses an additional channel to send a hashed authentication message for each original CAN message. Even though the CAN protocol modifications are not significant, the need of an additional channel still increases the cost of operation.

The idea of sending one and three authentication codes along with each original CAN message was proposed respectively in [19] and [20]. Although, no modification is needed to the CAN protocol, the network is still vulnerable to attacks like *Sniffing* and *Replay*, as the messages are not encrypted.

To the best of our knowledge, this is the first work that combines in-vehicle sensors and secure CAN network communications to achieve safe, collision-free braking at separations of 1 meter.

III. Background

A. Cooperative Driving through In-Vehicle Sensors

In our work, we consider two vehicles participating in cooperative driving with one of the vehicles following the other at a 1-meter separation. We consider the braking scenario and demonstrate secure and safe operation based on short-range radars and secure in-vehicle network communications.

Since in-vehicle sensors are used rather than wireless communication, data can be sampled at a much faster rate than the period of wireless message broadcast. The lead vehicle's deceleration, velocity, and current position can be communicated over the in-vehicle network (at the trail vehicle) to the brake controller, and the brake commands can be sent to the actuators as shown in Fig. 1. The methodology for securing the in-vehicle network is presented in the next section.

B. Securing In-Vehicle Network Communications

Advanced Encryption Standard (AES) is a popular and efficient symmetric-key encryption standard [21]. This, when combined with *Authentication* ensures both security as well as authenticity. Offset Codebook Mode (OCB) is an efficient AES mode of operation for authenticated encryption. OCB uses a counter to avoid diffusion [22] [23] and, as a result, is safe against replay attacks [24], where any messages on CAN can be recorded and resent later by a malicious node.

As shown in Fig. 2, a counter nonce is used to generate the Δ, which with the help of a symmetric encryption key is

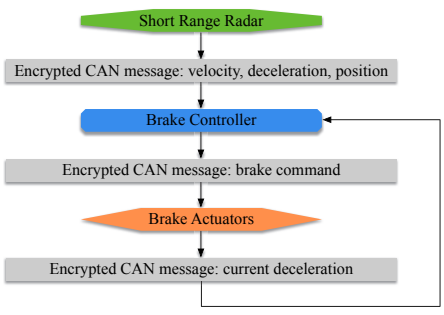

Fig. 1. Data Flow between Sensor, Controller, and Actuators

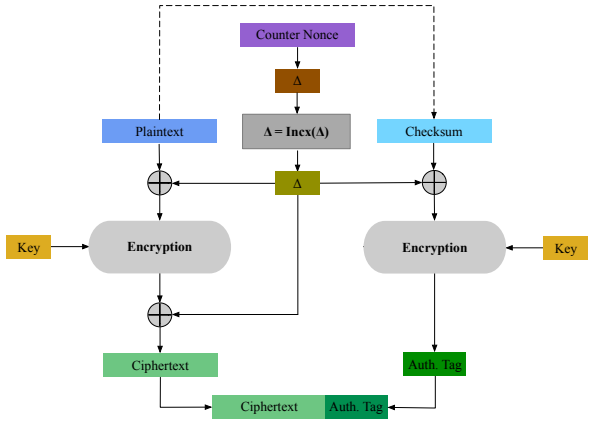

Fig. 2. AES - OCB encryption workflow

used to generate a ciphertext and an authentication tag from plaintext and checksum (generated from plaintext). However, due to the limited bandwidth of CAN, only the first 64 bits of the authentication tag is used in our work [25].

Additionally, we use AES - OCB for securing our CAN network communications. We employ fixed padding for the payload in each CAN frame, thereby, resulting in 16 bytes of padded payload which is then encrypted into 2 CAN frames (due to CAN's limited payload per frame). In addition, before transmission, an authentication frame of 64 bits is appended resulting for every CAN frame, in three frames that need to be sent on the bus.

Once a node receives all three frames, it uses the symmetric key to decrypt the ciphertext and removes the padding to restore the original 8 bytes of payload. Also, the authenticity of the sender is checked by decrypting the authentication frame. Clearly, this requires that the corresponding symmetric key and the counter nonce combination, unique to a particular message, be stored in the local persistent memory of each node.

Even though, AES - OCB secures communication, the resulting delay due to transmitting 3 frames for every CAN message can be very high for those messages featuring lower priority. Therefore, in this setting, if the brake messages are not/cannot be assigned high priorities, collisions may happen as shown later. An alternative as devised in this paper is presented in the next section.

IV. Dynamic Encryption Switching Scheme

In this section, we propose a workaround for networks where higher priorities cannot be assigned to messages related to braking. Counter Mode (CTR) [26] uses a secret counter against diffusion, and, uses a symmetric key to encrypt this counter before generating ciphertext as shown in Fig. 3.

Even though AES - CTR does not support authentication, it encrypts every CAN message in the same frame itself. Therefore, instead of 3 frames for every CAN message as in AES - OCB, now, only a single encrypted frame is sent. This considerably reduces the delay overhead for all messages.

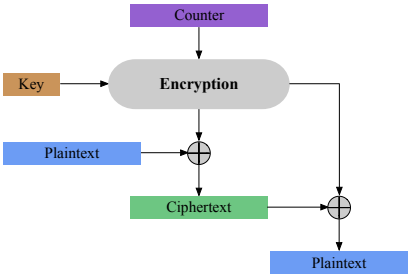

Fig. 3. AES - CTR encryption / decryption workflow

From the implementation perspective of cooperative driving, in the cruise situation, the ECU nodes, sensors and actuators can rely on AES - OCB for secure communications. However, once braking begins, all the nodes switch to and communicate using AES - CTR. At the CAN network level, this switching scheme can be easily accomplished by transmitting a message with a particular ID.

V. Evaluation

In this section, we evaluate the proposed encryption switching based on a mixed simulation/implementation setting as detailed below.

A. Evaluation Setup

1) Hardware, Propagation, Encryption and Decryption Delays: Once the data is generated by an ECU node, there is a delay due to encryption and/or authentication, as well as hardware delay. Further, once the corresponding message wins arbitration on the bus, there is a propagation delay in transmitting the encrypted CAN frame(s) on the bus. At the receiving node, again, after these aforementioned delays, the ECU can process the message.

To better estimate these delays, we employ Arduino Uno boards and their associated CAN-BUS Shields. In particular, we consider that every CAN frame carries 8 bytes of data. Based on this, the combined hardware and propagation delay was measured to be 375 μs. Both AES - OCB and AES - CTR were implemented on the Arduino Uno boards. In case of AES - OCB, the measured encryption / authentication delay was approximately 2 ms and so was the measured decryption / authentication delay. However, for AES - CTR, the observed encryption and decryption delays were 1 ms each. [1] The CAN bus transmission speed was set to be 1 $Mbps$.

2) Contention delay on the CAN bus: We simulate a shared in-vehicle CAN network of 30 nodes in OMNeT++ using an available CAN simulator [27]. These nodes represent sensors, actuators and ECUs not just belonging to our application, but also other hard real-time applications. The periods of messages sent by these nodes are in the 15 ms to 85 ms range. Further, the well-known rate-monotonic scheme was used to assign periods for the message set, i.e., the shorter the generated message period, the higher the assigned priority.

[1] Note that encryption/decryption delays can be shortened through parallel computations, but this is not considered here.

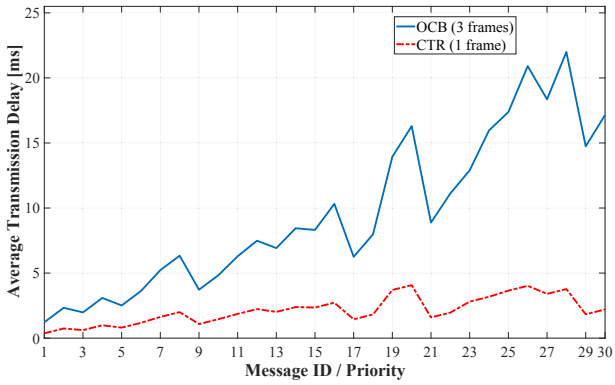

Fig. 4. Average transmission delay for encrypted CAN message using OCB (3 frames) and CTR (1 frame) encryption

If encryption and authentication are not implemented, the total bus utilization of this network is around 30%. However, implementing them, increased the utilization to around 90%. Note that, even with this increase, none of the messages miss their respective deadlines. Around 20,000 messages were exchanged during the whole simulation.

B. Test Results

1) Average and Measured Longest Transmission Delays: The average and measured longest transmission delays for all the 30 CAN messages encrypted using AES - OCB and AES - CTR are shown in Fig. 4 and Fig. 5 respectively. Clearly, due to the transmission of 3 frames for every CAN message, the delay values when using AES - OCB are larger when compared to AES - CTR. In fact, for higher-priority messages, the differences between these two are less. However, as the priority reduces, they become more significant. This can be reasoned by the fact that lower-priority messages have to compete with other higher-priority messages.

With respect to AES - CTR, even for lower-priority messages, both the average and measured longest transmission delays are lower when compared to AES - OCB. This is due

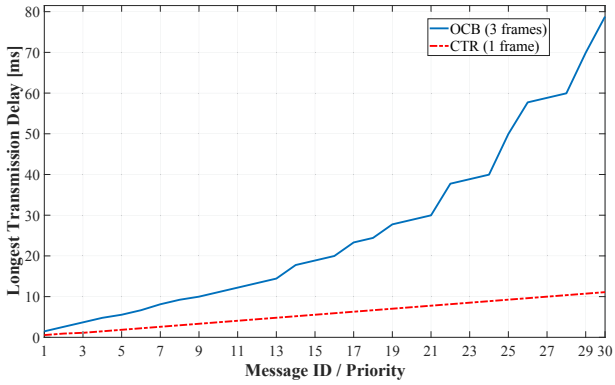

Fig. 5. Measured longest transmission delay for encrypted CAN message using OCB (3 frames) and CTR (1 frame) encryption

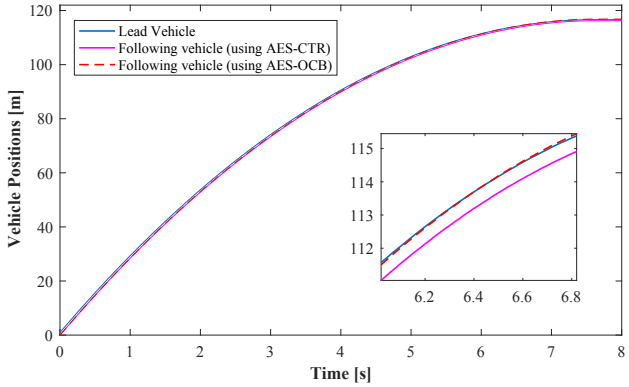

Fig. 6. Collision vs. Collision-free Braking

to encrypting a CAN message without needing more than one frame. One the other hand, as discussed above, AES - OCB is more secure than AES - CTR.

2) Cooperative Driving of Two Vehicles: The two vehicles are traveling at a cruise speed of $30\,m/s$ when the lead vehicle initiates braking and begins to decelerate at the rate of $4\,m/s^2$. This is sensed by the short-range radar of the following vehicle, and thus, communicates the same to the brake controller.

However, if the braking-related messages between radar, controller and actuator are assigned IDs 15, 16 and 17 respectively, then, due to the measured longest delays using AES - OCB, braking command takes around $50\,ms$ to reach the actuators, and hence, collision happens as shown in Fig. 6. However, if AES - CTR is used, then, this delay reduces to less than $20\,ms$ leading to no collision. This makes evident that we can use a high-security scheme such as AES - OCB, but we will have to switch temporarily to a less secure approach to meet safety constraints (when braking). Once the braking maneuver is over, we can switch back to the high-security approach. This way, we can reduce the time of higher vulnerability of the system to least possible.

VI. Conclusion

In this paper, we considered the braking scenario in cooperative driving with inter-vehicle distances of only 1 meter. We make use of in-vehicle sensors and secure in-vehicle network communications. The advantages include optimum fuel savings, and also security from external cyberattacks. However, the security overhead poses the risk of vehicle collisions, if the related messages are not assigned the highest priorities, which may not always be possible due to other important messages on the bus. Hence, we proposed an encryption switching scheme that reduces the overall delay to collision-free braking, while still guaranteeing a sufficient level of security. As part of future work, we plan to extend our architecture to larger platoons with heterogeneous vehicle deceleration capabilities.

References

[1] C. Bergenhem, and Q. Huang, and A. Benmimoun, and T. Robinson, "Challenges Of Platooning On Public Motorways," 2019.

[2] H. Fritz, "Longitudinal and lateral control of heavy duty trucks for automated vehicle following in mixed traffic: experimental results from the CHAUFFEUR project," in *Proceedings of the IEEE International Conference on Control Applications*, 1999.

[3] G. Xu, and L. Liu, and Y. Ou, and Z. Song, "Dynamic Modeling of Driver Control Strategy of Lane-Change Behavior and Trajectory Planning for Collision Prediction," *IEEE Transactions on Intelligent Transportation Systems*, 2012.

[4] M. Michaelian, and F. Browand, "Field Experiments Demonstrate Fuel Savings for Close-Following," 2000.

[5] M. Zabat, and N. Stabile, and S. Farascaroli, and F. Browand, "The Aerodynamic Performance Of Platoons: A Final Report," *Research Reports, Working Papers, Proceedings, Institute of Transportation Studies, UC Berkeley*, 1995.

[6] *IEEE 802.11p Part11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Amendment 7: Wireless Access in Vehicular Environment*, IEEE Std., 2010.

[7] *Intelligent Transport Systems (ITS); Access layer specification for Intelligent Transport Systems using LTE Vehicle to everything communication in the 5,9 GHz frequency band*, European Telecommunications Standards Institute Std., 2018.

[8] *Intelligent Transport Systems(ITS); European profile standard for the physical and medium access control layer of Intelligent Transport Systems operating in the 5 GHz frequency band*, European Telecommunications Standards Institute Std., 2010.

[9] C. Miller and C. Valasek, "Adventures in Automotive Networks and Control Units," in *DEF CON 21 Hacking Conference*, 2013.

[10] C. Miller and C. Valasek, "A Survey of Remote Automotive Attack Surfaces," in *Black Hat USA*, 2014.

[11] S. Linsenmayer, and D. V. Dimarogonas, and F. Allgöwer, "Nonlinear event-triggered platooning control with exponential convergence," *International Federation of Automatic Control*, 2015.

[12] A. Borri and D.V. Dimarogonas and K.H. Johansson and M.D. Di Benedetto and G. Pola, "Decentralized symbolic control of interconnected systems with application to vehicle platooning," *International Federation of Automatic Control Proceedings Volumes*, vol. 46, pp. 285–292, 2013.

[13] V. Turri and B. Besselink and J. Mårtensson and K. H. Johansson, "Fuel-efficient heavy-duty vehicle platooning by look-ahead control," in *53rd IEEE Conference on Decision and Control,*, 2014.

[14] D. Swaroop and J. K. Hedrick, "String stability of interconnected systems," in *Proceedings of the American Control Conference*, 1995.

[15] D. K. Murthy and A. Masrur, "Exploiting space buffers for emergency braking in highly efficient platoons," in *IEEE International Conference on Embedded and Real-Time Computing Systems and Applications*, 2017.

[16] A. Vinel, and N. Lyamin, and P. Isachenkov, "Modeling of V2V Communications for C-ITS Safety Applications: A CPS Perspective," *IEEE Communications Letters*, 2018.

[17] B. Groza, and S. Murvay, and A. van Herrewege, and I. Verbauwhede, "LiBrA-CAN: A Lightweight Broadcast Authentication Protocol for Controller Area Networks," in *International Conference on Cryptology and Network Security*, 2012.

[18] O. Hartkopp, C. Reuber and R. Schilling, "MaCAN - Message authenticated CAN," in *Escar Conference on Embedded Security in Cars*, 2012.

[19] H. U. et al., "Security authentication system for in-vehicle network," *SEI Technical Review*, 2015.

[20] Z. King and S. Yu, "Investigating and securing communications in the Controller Area Network (CAN)," in *International Conference on Computing, Networking and Communications*, 2017.

[21] J. Daemen and V. Rijmen, *The Design of Rijndael*, 2002.

[22] C. E. Shannon, "Communication Theory of Secrecy Systems," *Bell Systems Technical Journal*, 1949.

[23] S. William, *Cryptography and Network Security*, 2014.

[24] P. Syverson, "A Taxonomy of Replay Attacks," *7th IEEE Computer Security Foundations Workshop*, 1999.

[25] P. Rogaway, and M. Bellare, and J. Black, and T. Krovetz, "OCB: A Block-Cipher Mode of Operation for Efficient Authenticated Encryption," in *ACM Transactions on Information and System Security*, 2001.

[26] W. Diffie and M. E. Hellman, "Privacy and Authentication: An Introduction to Cryptography." 1979.

[27] J. M. et al., "A Simulation Environment based on OMNeT++ for Automotive CANEthernet Networks," in *4th International Workshop on Analysis Tools and Methodologies for Embedded and Real-time Systems*, 2013.