**Short Abstract – 200 words:**

We propose Mini-MAC, a new message authentication protocol that works in existing automotive computer networks without delaying any message or increasing network traffic.

Deployed in many vehicles, the CAN bus is a low-speed network connecting electronic control units, including those that control critical functionality. The CAN bus is extremely vulnerable to malicious actors with bus access, including wireless. Traditionally, Message Authentication Codes (MACs) help authenticate the sender of a message, and variants prevent message replay attacks; however, standard MACs are unsuitable for use on the CAN bus because of small payload sizes. Restrictions of the CAN bus severely limit how well this network can be protected.

Mini-MAC is based on a counter-seeded keyed-Hash MAC (HMAC), augmented with message history and truncated to fit available message space. It does not increase bus traffic and incurs a very small performance penalty relative to the provably secure HMAC. It is the first proposal to combine these two tenets for vehicle networks. The message history feature protects against all transient attackers, even if they know the keys. Though the CAN bus cannot be properly secured against a dedicated attacker, Mini-MAC meaningfully raises the bar of vehicular security, enhancing the safety of drivers and others.

**(Original – 217 words):**

We propose Mini-MAC, a new message authentication protocol that works in existing automotive computer networks without delaying any message or increasing network traffic.

Deployed in many vehicles, the CAN bus is a low-speed network connecting electronic control units, including those that control critical functionality such as braking and acceleration. The CAN bus is extremely vulnerable to malicious actors with bus access, including wireless access. Traditionally, Message Authentication Codes (MACs) help authenticate the sender of a message, and variants prevent message replay attacks; however, standard MACs are unsuitable for use on the CAN bus because of small payload sizes. Restrictions of the CAN bus, including the need not to delay messages or increase bus traffic, severely limit how well this network can be protected.

Mini-MAC is based on a counter-seeded keyed-Hash MAC (HMAC), augmented with message history and truncated to fit available message space. It does not increase bus traffic and incurs a very small performance penalty relative to the provably secure HMAC. It is the first proposal to combine these two tenets for vehicle networks. The message history feature protects against all transient attackers, even if they know the keys. Though the CAN bus cannot be properly secured against a dedicated attacker, Mini-MAC meaningfully raises the bar of vehicular security, enhancing the safety of drivers and others.