AutoSec 2019
Dallas, TX, USA

TOUCAN:
A proToCol tO secUre Controller Area Network

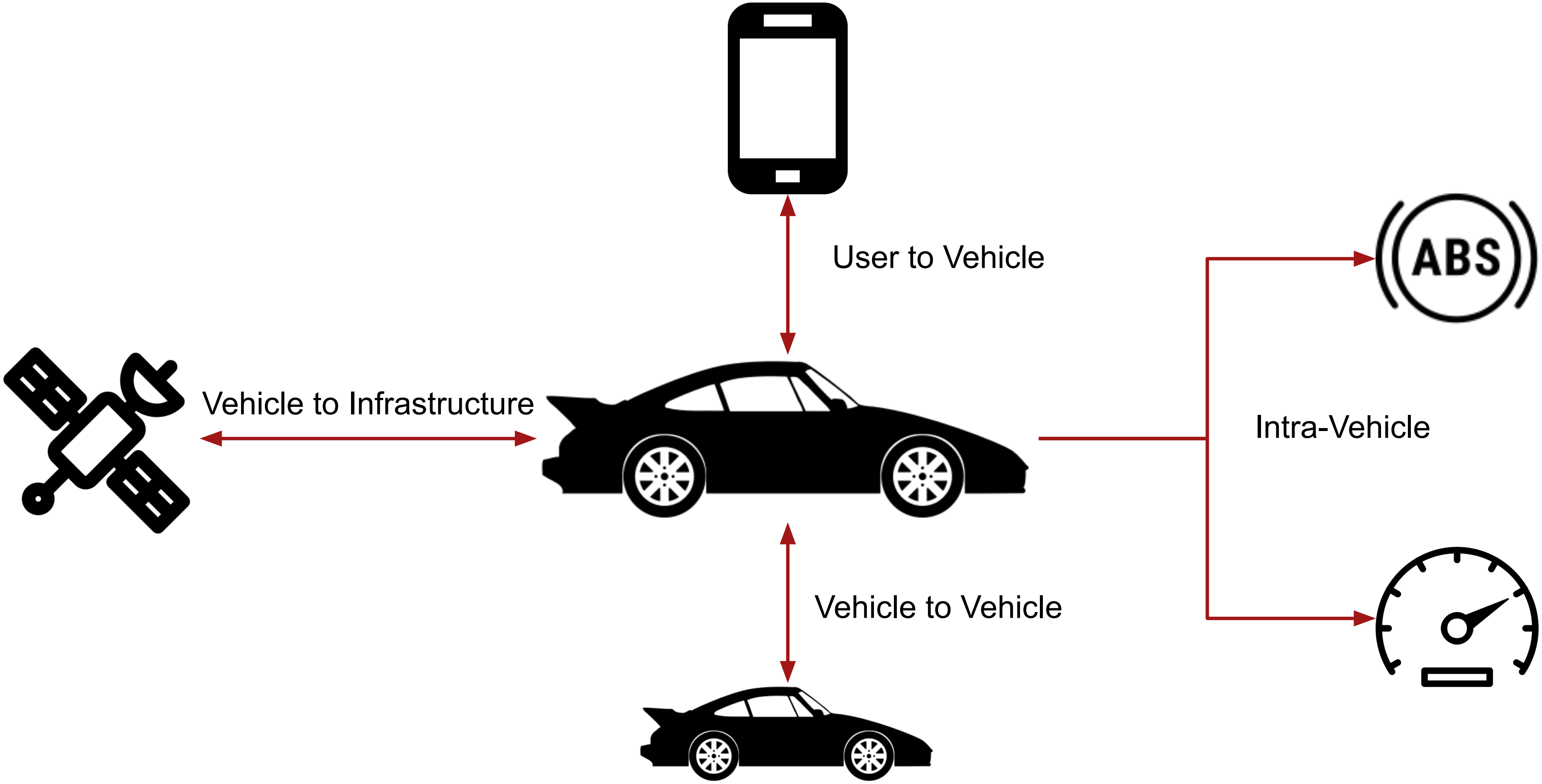
Giampaolo Bella

Pietro Biondi

Gianpiero Costantino

Ilaria Matteucci

Automotive communication domains



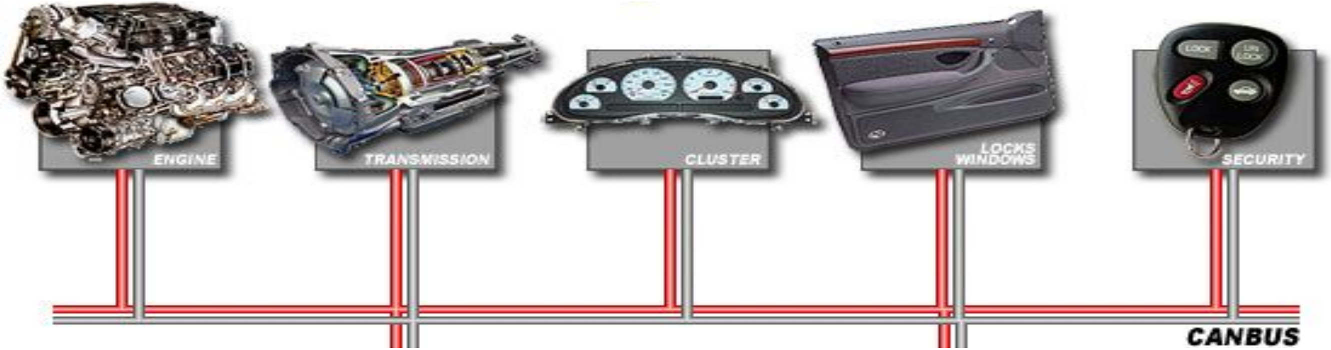
User to Vehicle

Vehicle to Infrastructure

Intra-Vehicle

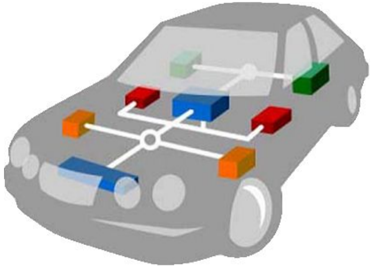
Vehicle to Vehicle

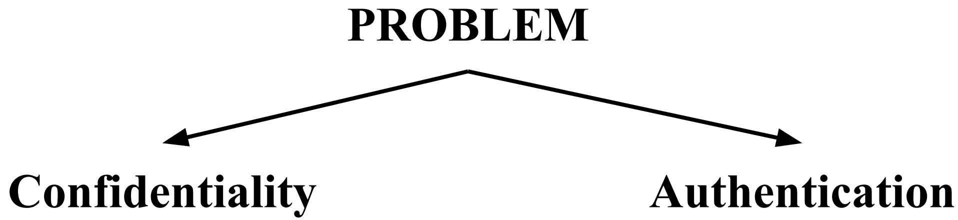
Controller Area Network



The **Controller area network (CAN-bus)** is provided with:

- Serial communication protocol
- Message anti-collision protection
- Error detection





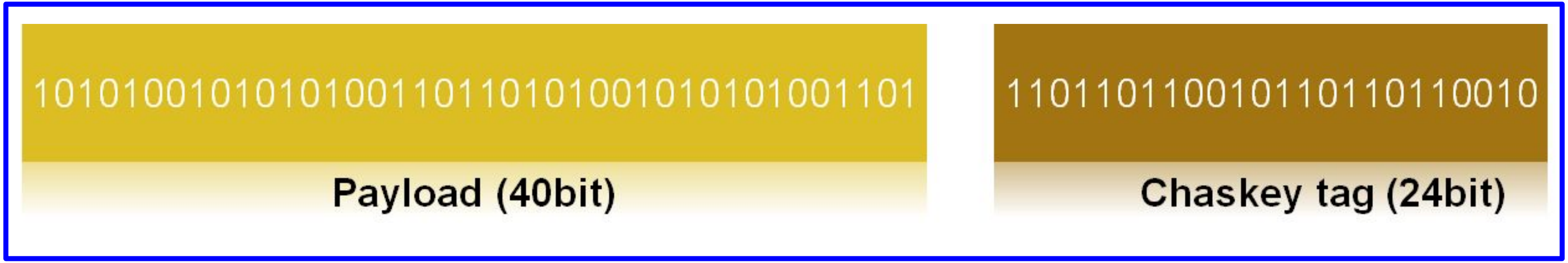
PROBLEM

Confidentiality

Authentication

TOUCAN Frame

Turning CAN frames into *TOUCAN* frames



SPECK-64

SPECK-64 + Chaskey MAC

SPECK-64: Symmetric cipher used in systems with low computational resources.

The features of SPECK are:

- Block cipher with 64-bit block size
- Supported key lengths: 128, 192 and 256 bit
- Efficiency in software and hardware
- On the ARM platform: about 3 times faster than AES

Chaskey: permutation-based MAC algorithm based on Addition-Rotation-XOR (ARX) with some useful features:

- Efficient MAC algorithm for microcontrollers
- It is intended for applications that require 128-bit security
- Robustness under tag truncation

Design evaluation

TOUCAN reduce the payload carried per frame. This decreases the number of messages that the car manufacturer can leverage to implement modern services based on communication among ECUs.

Although, we argue that a message space of 2^40 is sufficient, this will have to be validated over time as more and more developed applications appear.

Risk analysis

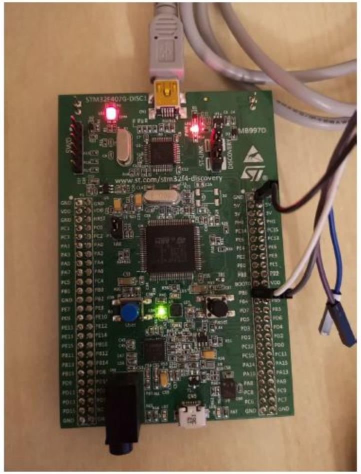
- **Risk of guessing the tag**. According to Chaskey, the probability of constructing a forgery by guessing the tag is $2^{-tag\_len} = 2^{-24} = 0.6 * 10^{-7}$

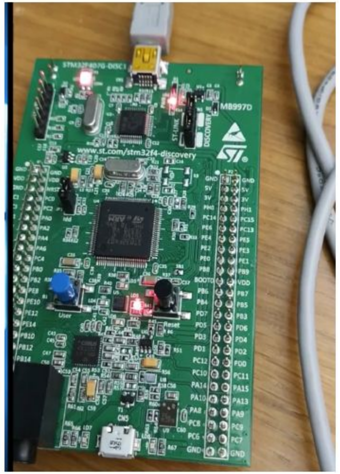
- **Probability of tag collisions.** The collision probability depends on both the MAC length and the number of times the MAC is calculated: $2^{\frac{tag\_len}{2}} = 2^{\frac{24}{2}} = 2^{12} = 4096$

- **Security of SPECK 64/128.** No attacks found with 27 rounds

A prototype implementation of TOUCAN

- **STM32F407 Discovery**
- **Green led:** the payload is correctly hashed / encrypted
- **Red led:** the payload is not correctly hashed / encrypted





Performances

Algorithm	**Board Speed** [MHz]	**Time** [µs]
Chaskey MAC	168	0,43
SPECK-64	168	5,36
SPECK-64 + Chaskey MAC	168	5,79

Comparison with the related work

F1 Standard CAN: Conform to size and contents as they are specified by the CAN standard

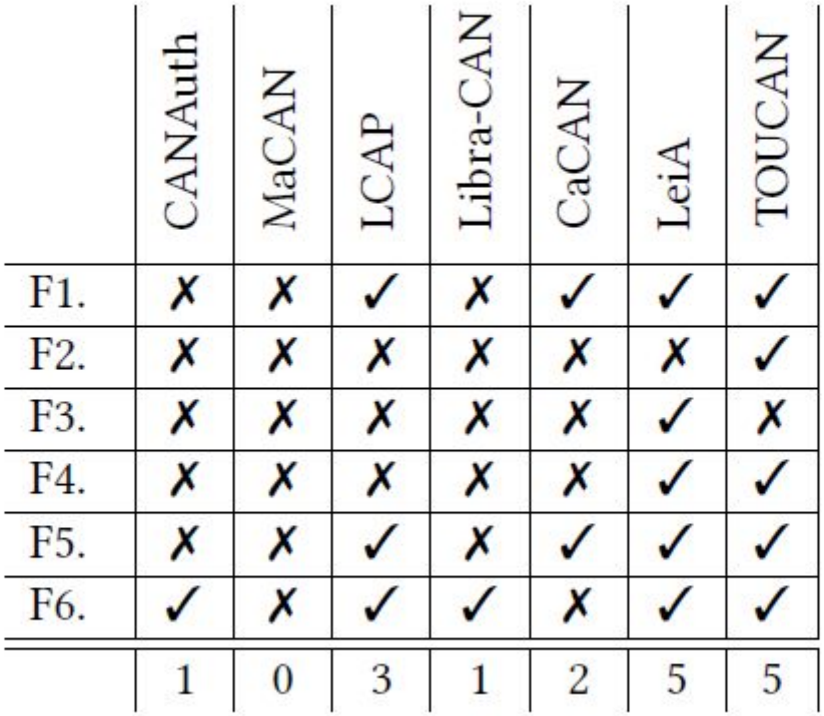
F2 Frame rate equal to CAN's: When the protocol that does not need to send more frames than CAN does

F3 Payload size not smaller than CAN's: This holds of a protocol that preserves the standard CAN size of 64 bits for the payload size

F4 Standard AUTOSAR: Protocol compliant with the AUTOSAR standard

F5 No ECU hardware upgrade: When the protocol requires no upgrade to the ECUs

F6 No infrastructure upgrade: Concerns the network and the overall infrastructure that supports the protocol



	CANAuth	MaCAN	LCAP	Libra-CAN	CaCAN	LeiA	TOUCAN
F1.	✗	✗	✓	✗	✓	✓	✓
F2.	✗	✗	✗	✗	✗	✗	✓
F3.	✗	✗	✗	✗	✗	✓	✗
F4.	✗	✗	✗	✗	✗	✓	✓
F5.	✗	✗	✓	✗	✓	✓	✓
F6.	✓	✗	✓	✓	✗	✓	✓
	1	0	3	1	2	5	5

Conclusions

❑ Prototype implementation of TOUCAN, a protocol to secure CAN communication against an active eavesdropper in an AUTOSAR compliant way

❑ TOUCAN needs only the update of the firmware of existing ECUs but demands no hardware upgrade to the network

❑ It is based on fast hashing and symmetric encryption with the aim of ensuring authenticity, integrity and confidentiality

❑ Cryptographic functions never exceed six microseconds

❑ Payload size to 40 bits but this is largely sufficient for all control traffic

Future Works

- Secure distribution of cryptographic keys that are necessary to bootstrap both the hashing and the encryption primitives

- Simulation of an in-vehicle network by having at least two ECUs communicate securely between each other

- The precise evaluation of the extent to which more expensive and performing boards than the STM32F407 Discovery used here can reduce the runtimes

AutoSec 2019
Dallas, TX, USA

Thank you for your attention

Giampaolo Bella
giamp@dmi.unict.it

Pietro Biondi
pietro.biondi94@gmail.com

Gianpiero Costantino
gianpiero.costantino@iit.cnr.it

Ilaria Matteucci
ilaria.matteucci@iit.cnr.it

Find us on:
https://sowhat.iit.cnr.it/
Security Of the Way to Handle Automotive sysTems