ADAPTABLE SAFETY AND SECURITY IN V2X SYSTEMS

Miguel Villarreal-Vazquez[1], Bharat Bhargava[1], Pelin Angin[2]

[1] Department of Computer Science, Purdue University

[2] Department of Computer Engineering, Middle East Technical University

Acknowledgments: This publication was made possible by NPRP grant # [7-1113-1-199] from the Qatar National Research Fund (a member of Qatar Foundation). The statements made herein are solely the responsibility of the authors. The authors would also like to thank Dr. Weichao Wang and Dr. Leszek Lilien for their valuable comments and discussions.

MOTIVATION

- Vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) networks, i.e.V2X systems (Internet of vehicles) receiving increased attention because of significant contribution to improving safety
- V2X systems hot targets for attackers trying to exploit software vulnerabilities → Compromised security, privacy and safety
- V2V system needs security to ensure the trustworthiness of communication between vehicles
- The source of each message needs to be trusted and message content needs to be protected from outside interference

ISSUES WITH EXISTING V2X SAFETY AND SECURITY APPROACHES

- Safety, security and performance considered separately for V2X systems
- Networking services have critical shortcomings, hurting time-critical safety applications
- V2X research based on unrealistic conditions/limited operating conditions
- Static selection of security, networking and safety features

FOCUS

- Developing a systematic approach to figure out:
  - ✓ How V2X technologies increase safety
  - ✓ How much the use of secure communication negatively affects safety
- Security versus safety analysis
  - ✓ Categories of safety messages
  - ✓ Semantics of safety messages
  - ✓ Different driving scenarios
  - ✓ Examples: Highways, Streets on populated areas, Traffic lights
- Developing an adaptive security model for V2X networks that changes the configuration of the secure channel based on sensitivity, context, safety level

CATEGORIES OF SAFETY MESSAGES

- **Traffic information messages**: Used to disseminate the current conditions of specific areas and they indirectly affect safety

- **General safety messages**: Used for cooperative driving and collision avoidance, and require an upper bound on the delivery delay of messages

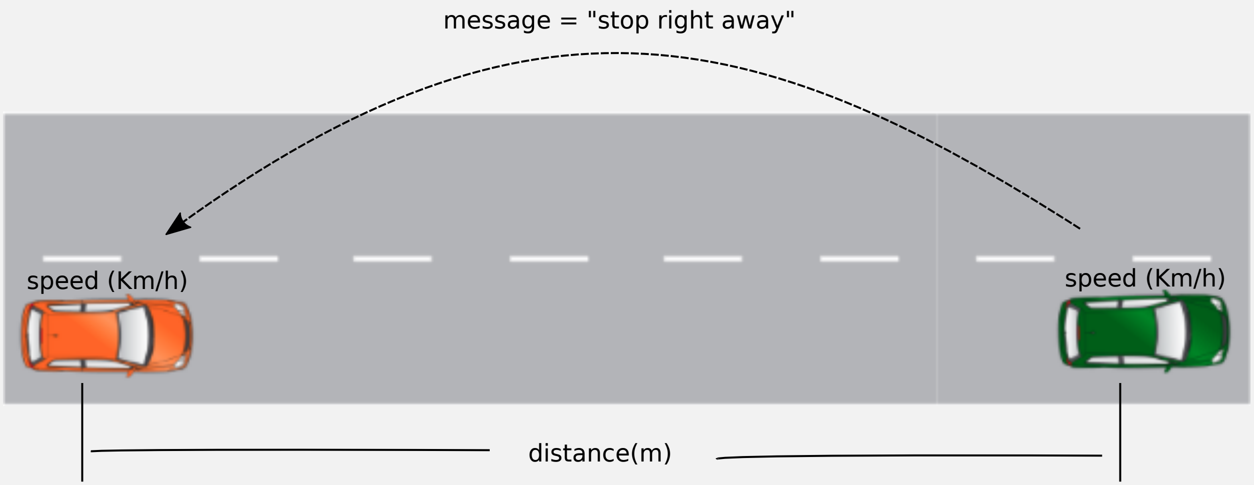
- **Liability-related messages**: Exchanged after an accident occurs

Our target: Critical-time messages!

DRIVING SCENARIO

Scenario 1: Sudden stop on a highway

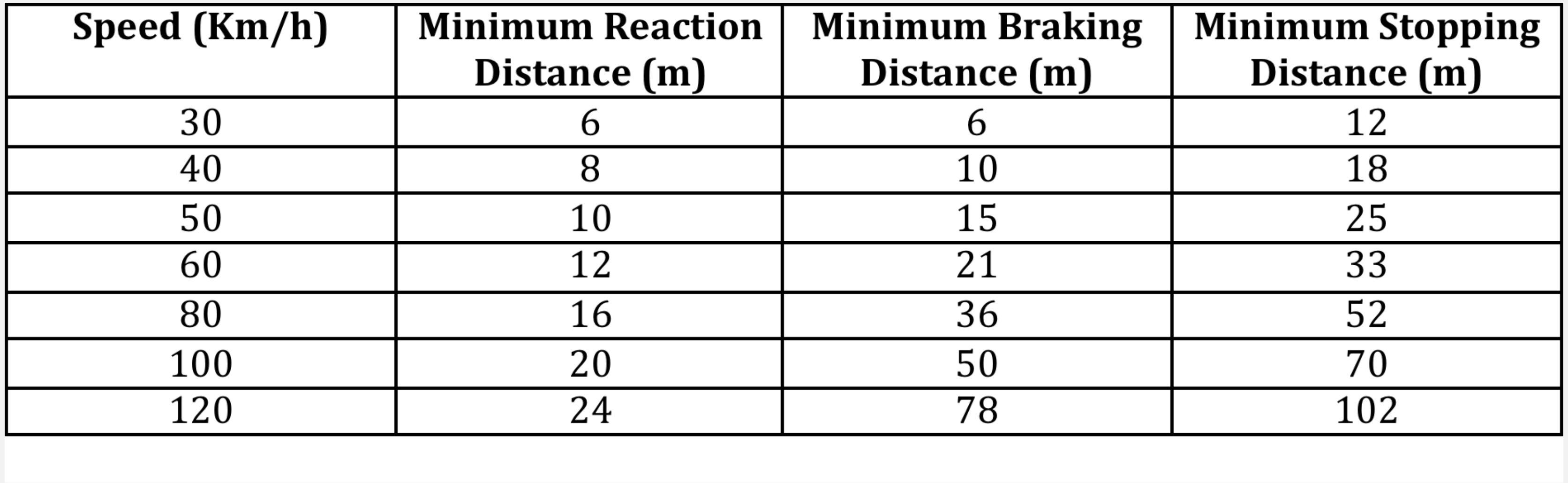
- Vehicles move at same speed on the highway
- Pre-determined distance between them
- Reaction time with and without V2V
- Reaction time with secured V2V



DRIVING SCENARIO

Stopping distance:

- Driver's perception time
- Driver's reaction time
- Vehicle's reaction time
- Vehicle's braking capability



Speed (Km/h)	Minimum Reaction Distance (m)	Minimum Braking Distance (m)	Minimum Stopping Distance (m)
30	6	6	12
40	8	10	18
50	10	15	25
60	12	21	33
80	16	36	52
100	20	50	70
120	24	78	102

The RSA recommended minimum stopping distance under dry conditions

SYSTEM MODEL

- Network:
  - ✓ IEEE 802.11a compliant
  - ✓ 6Mbps minimum

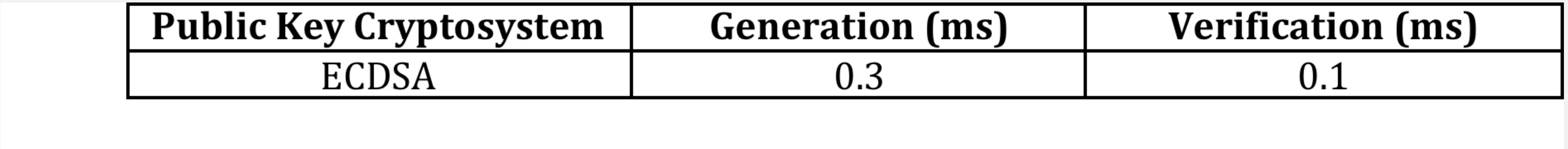
- Security mechanism on V2V:
  - ✓ PKI infrastructure
  - ✓ Every vehicle is assigned a public and private key
  - ✓ Public key distributed through a certificated signed by the CA
  - ✓ Authenticated message:

$$M_{AUTH} = \langle (M|T), Sign(M|T), Cert_{CA\ SIGNED} \rangle$$

SYSTEM MODEL

- Security costs on V2V:

✓ Processing cost



Public Key Cryptosystem	Generation (ms)	Verification (ms)
ECDSA	0.3	0.1

Signature generation and verification times

✓ Communication cost:

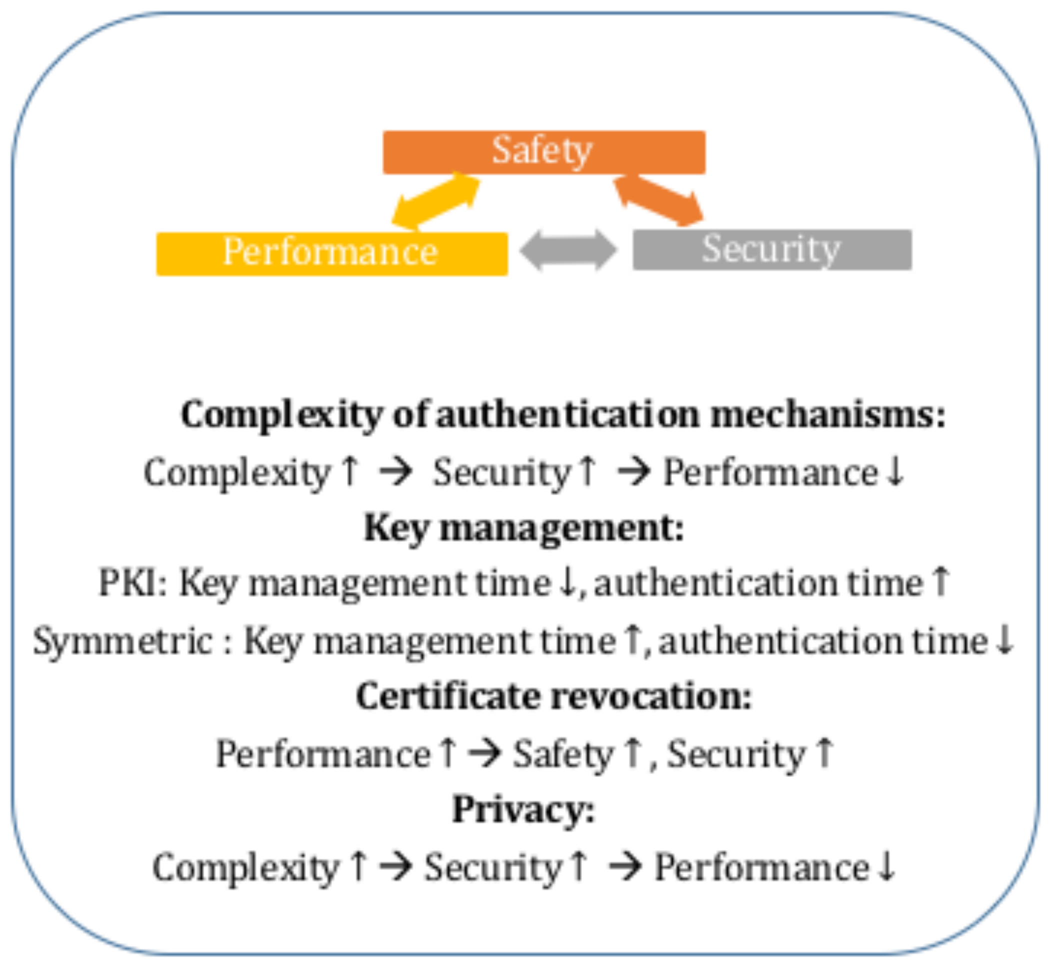
$$d_{com} = d_{transmission} + d_{propagation} + d_{queueing}$$

▪ Distance: 120m

▪ Bandwidth: 6Mbps

▪ Speed of communication link: 3x10^8m/s

SAFETY-SECURITY TRADEOFFS



Complexity of authentication mechanisms:

Complexity ↑ → Security ↑ → Performance ↓

Key management:

PKI: Key management time ↓, authentication time ↑

Symmetric : Key management time ↑, authentication time ↓

Certificate revocation:

Performance ↑ → Safety ↑ , Security ↑

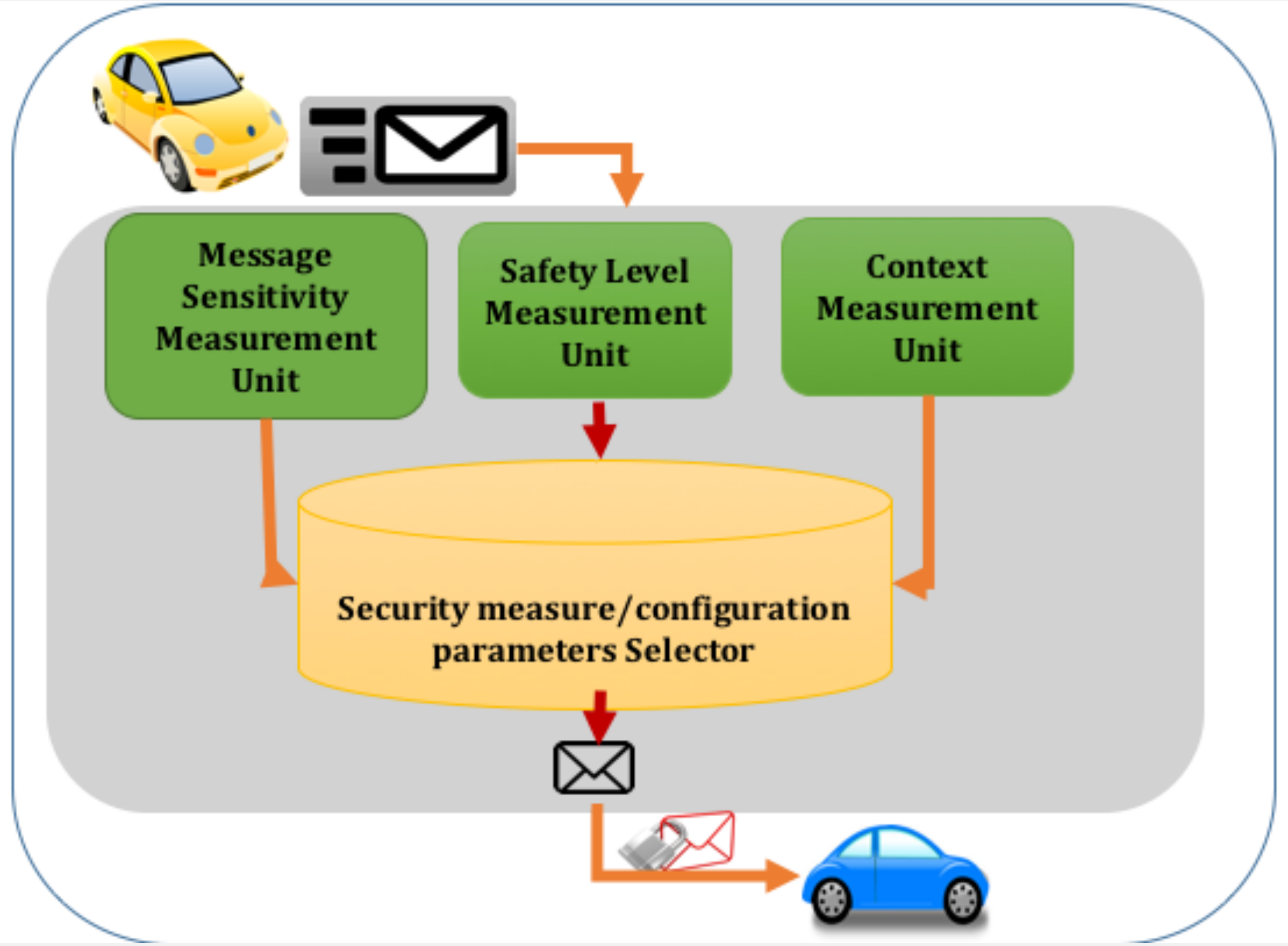
Privacy:

Complexity ↑ → Security ↑ → Performance ↓

ADAPTABLE SAFETY/SECURITY APPROACH

- Self-adaptive software solutions capable of adjusting behavior at runtime to achieve functional or QoS goals
- Self-protecting software detecting security threats and mitigating through runtime adaptation techniques
- Monitoring activity needs to be isolated from V2X system activities → same resources used
- AOP to monitor software behavior and adapt

ADAPTABLE SECURITY MODEL


Message Sensitivity Measurement Unit
Safety Level Measurement Unit
Context Measurement Unit
Security measure/configuration parameters Selector

ADAPTABLE SECURITY SYSTEM COMPONENTS

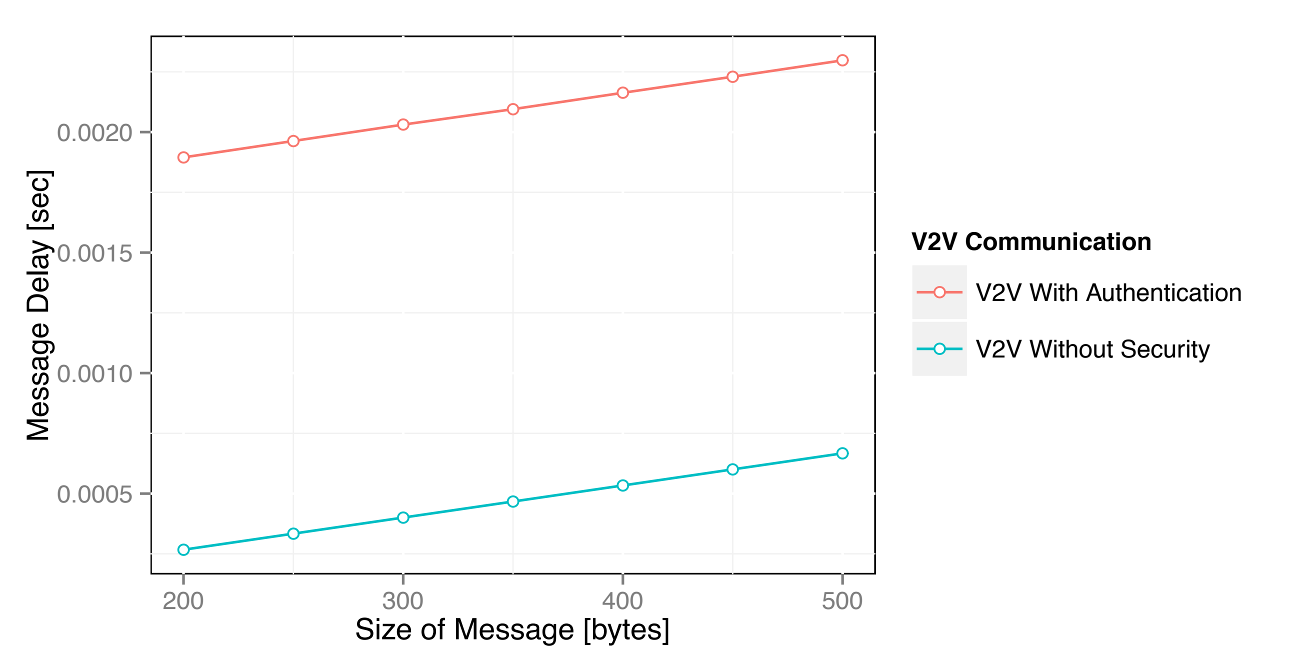
- ***Message sensitivity measurement unit***: Measures the security sensitivity of the messages.
- ***Safety level measurement unit***: Measures the instantaneous safety level of the vehicle based on the mobility of the vehicles, traffic congestions etc.
- ***Context measurement unit***: Measures the current network throughput, latency, and packet losses for the vehicle with respect to surrounding vehicles. Based on this information the configuration parameters of the secure channel are adapted dynamically.

PERFORMANCE METRICS

- Number of outgoing/incoming packets
- Signature generations/verifications per second
- Packet delays
- Transmission delays
- Message encryption/decryption delays
- Number of neighboring vehicles, RSUs
- Signal strength indicator
- …

EXPERIMENTS

- Experiment 1: Measurement of delays of V2V messages with and without security

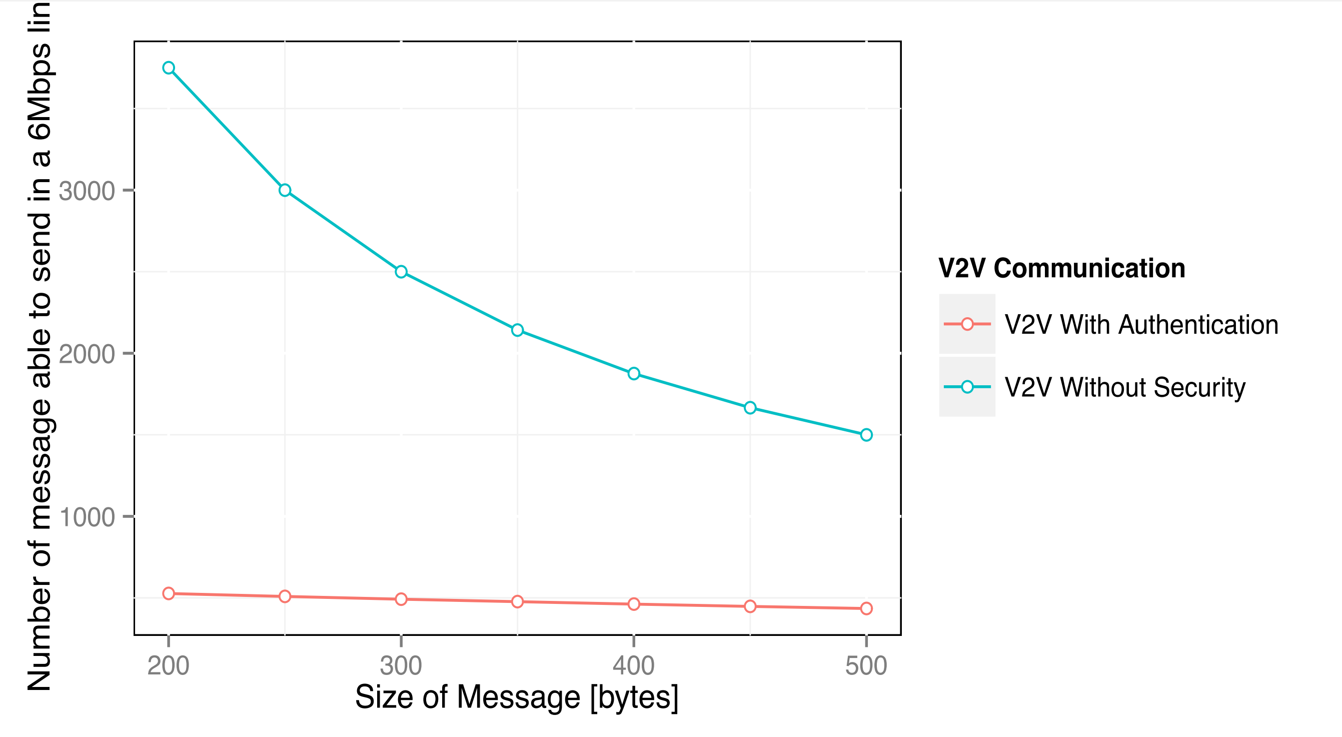


✓ Speed: 120Km/h

✓ Distance: 120m

EXPERIMENTS

- Experiment 2: Measurement of the capacity of the link

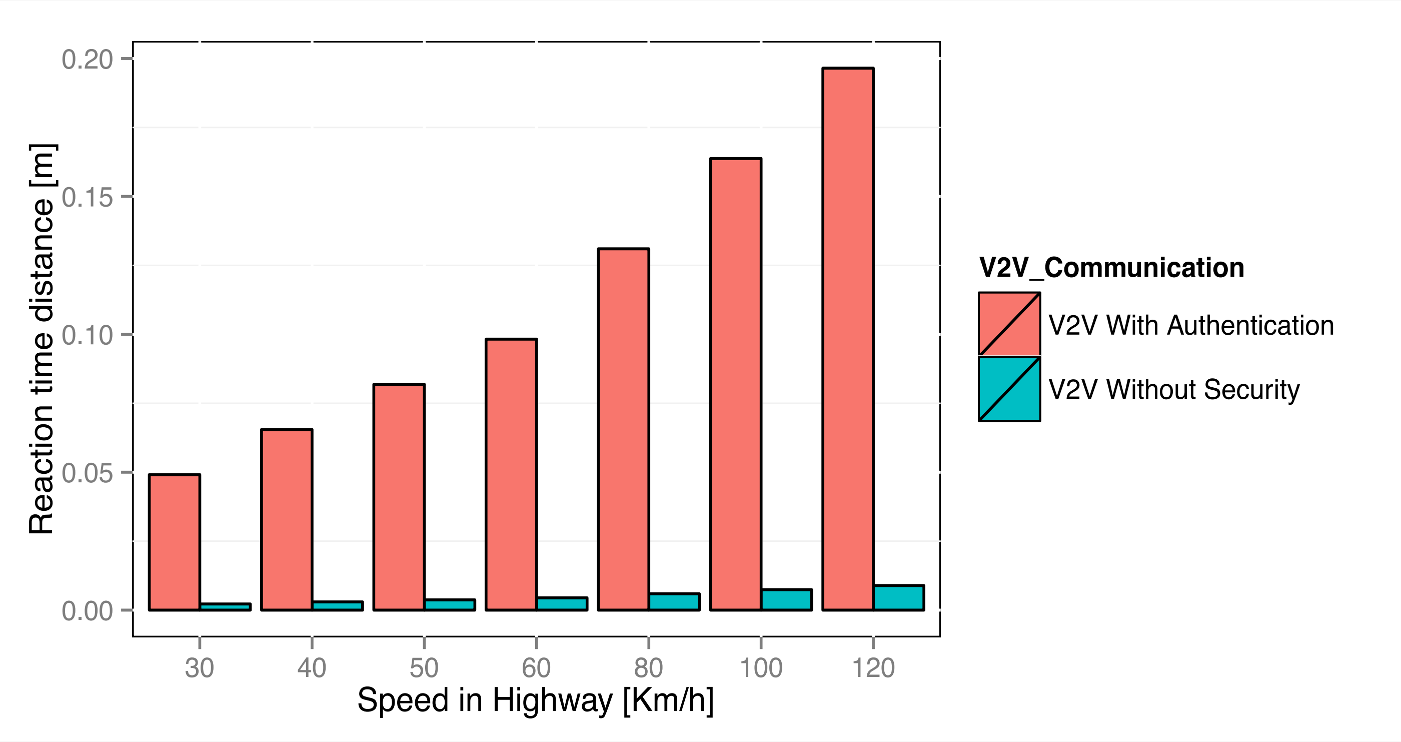


✓ Speed: 120Km/h

✓ Distance: 120m

EXPERIMENTS

- Experiment 3: Reaction time with V2V



✓ Size of message: 200 bytes

✓ Distance: 120m

FUTURE WORK

- Extended evalution with iTETRIS simulation platform under different scenarios and conditions
- Development of quantitative model of tradeoffs between safety/security/performance aspects
- Development of full adaptability framework