

Autonomous V2V: Security, Privacy, Safety

Bharat Bhargava

Professor in Computer Science Department, CERIAS
Purdue University, West Lafayette, IN, USA

Outline

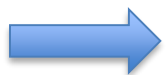
1. Problem Statement
2. Solutions
 - 2.1. Secure Intelligent Transportation System
 - 2.1.1. Secure inter-vehicle communication
 - 2.1.2. Encrypted Search over Encrypted Vehicle Records
 - 2.2.3. Vehicle Recognition
 - 2.2.4. On-the-fly Machine Learning Analytics
 - 2.2.5. Secure video transfer and face detection
 - 2.2. Security vs. Safety
3. Evaluation & Conclusions
4. Related Work

Motivation

- Intelligent Transport Systems (ITS) (aka. connected vehicles) are the key enabling technology to improve road safety & traffic efficiency
- By 2025, most vehicles will be equipped with powerful sensing capabilities and wireless-enabled on-board units (OBUs) enabling in-vehicle communications, vehicle-to-vehicle (V2V) communications and vehicle-to-infrastructure (V2I) communications
- Several applications including *cooperative adaptive cruise control, intersection collision warning, wrong way driving warning, remote diagnostic of vehicles etc.* will integrate V2X technologies

ITS Security Challenges

- **Data integrity and authenticity:** ITS entities should be able to verify the authenticity of received messages in order to prevent Sybil attacks
- **Data confidentiality:** All exchanged messages should be properly encrypted to prevent disclosure of sensitive information
- **Privacy and anonymity:** Identities of ITS users should not be easily identifiable from the exchanged messages
- **Traceability:** ITS authorities should be able to track malicious entities misusing the ITS systems
- **Real-time availability of information:** All exchanged information should be processed and made available in real-time, requiring the implementation of low-overhead and lightweight cryptographic algorithms
- **Robustness against external attacks:** ITS entities should be robust against external attacks such as denial-of-service or Sybil attacks, and ITS software should be almost free of vulnerabilities.



Need to achieve optimal tradeoff between security and performance to meet the quality of service requirements of ITS

Problem Statement

- Provide road assistance and road safety: Secure Intelligent Transportation System
 - Provide secure communications in V2X network
 - Support encrypted search over encrypted vehicle records
 - Support vehicle recognition
 - Perform decentralized on-the-fly machine learning analytics
 - Support face detection in video data, captured by dashed camera
- Measure impact of security mechanisms on safety
 - Develop a systematic approach for attack analysis
 - Dynamically monitor and adapt parameters

Solution Overview

- Provide secure communications in V2X network

Solution: use self-protected Vehicle Record (VR), based on extended Active Bundle (AB) [1], [2], [3] concept. VR incorporates:

- Key-value pairs in encrypted form
- Access control and metadata policies
- Policy enforcement engine

Example of key-value pair:

vr.drivingLicenseNumber : **Enc**(1234 56 7890)

Solution Overview

- Provide secure communications in V2X network
- VR provides:**
- Role-based and attribute-based access control which considers client's authentication method and browser cryptographic capabilities [4]
 - Prevention and detection of data leakages, made by insiders to unauthorized entities [6], [19]
 - Fast on-the-fly data analytics over encrypted data
 - Encrypted search over encrypted data, supporting large subset of SQL queries [11]
 - Tamper-resistance [2]

Solution Overview

- Encrypted Search over Encrypted Vehicle Records

Solution:

- Store encrypted database in cloud
- Use Homomorphic Encryption (HE)
- Use CryptDB database engine

Advantages:

- Database is protected against malicious or curious cloud administrators [11]
- Large subset of SQL queries is supported

Solution Overview

- Vehicle Recognition

Solution:

- Use **Sighthound** by Dehghan et al. [8]: a vehicle make, model, and color recognition (MMCR) system
- **Sighthound** relies on a deep convolutional neural network

Advantages:

- Performance: the total processing time to recognize vehicle's attributes and transfer them to cloud is around one second
- Accuracy about 92%

Solution Overview

- Decentralized on-the-fly Machine Learning Analytics

Solution:

- Create Vehicle Data Record (VDR) by adding extra-field “Summary” to VR
- Encrypt “Summary” with MMCR-key
- MMCR key is derived based on vehicle’s attributes: make, model, color. Sighthound [8] is used

Advantages:

- Analytics administrator, who has MMCR key, can quickly extract “Summary” field from VDR without going through policy evaluation process

Solution Overview

- Face detection is vehicle dash camera video

Solution:

- Split captured video into frames, i.e. into separate images
- Apply face detection algorithms to every frame [5]
- Mark those frames with faces detected
- Recompile separate video fragments: with and without human faces

Advantages:

- Face detection result can be used in access control policies since video fragments with human faces are more sensitive data and they are allowed to be accessed by restricted set of

Publications

1. D. Ulybyshev, S. Palacios, G. Mani, A. Alsalem, B. Bhargava, P. Goyal, “On-the-fly Analytics over Encrypted Records in Untrusted V2X Environments”, ICACEEE 2018, May 2018 (Accepted, in-press)
2. D. Ulybyshev, A. Alsalem, B. Bhargava, S. Savvides, G. Mani, L. Ben-Othmane, "Secure Data Communication in Autonomous V2X Systems", IEEE ICIOT, June 2018 (Accepted, in-press)
3. D. Ulybyshev, B. Bhargava, M. Villarreal-Vasquez, A. O. Alsalem, D. Steiner, L. Li, J. Kobes, H. Halpin, and R. Ranchal, “Privacy-preserving data dissemination in untrusted cloud,” in Cloud Computing (CLOUD), 2017 IEEE 10th Intl. Conf. on IEEE, 2017, pp. 770–773
4. M. Villarreal-Vasquez, B. Bhargava, P. Angin. "Adaptable Safety and Security in V2X Systems", IEEE ICIOT, June 2017
5. C. Qu, [D. Ulybyshev](#), B. Bhargava, R. Rohit, and L. Lilien. "[Secure Dissemination of Video Data in Vehicle-to-vehicle Systems](#)", DNCMS 2015

Vehicle as an Autonomous System

- Intelligent Autonomous Systems (IAS) such as Secured Intelligent Transportation Systems are characterized as
 - Highly **Cognitive**: Performs monitoring, recording data provenance, data analysis, learning, and decision making.
 - Effective in **Knowledge Discovery**: Identifies new patterns from raw data through advanced data analytics.
 - **Reflexive**: Swiftly adapts to changes in context
 - **Trusted**: Provides consensus, verifiability, and integrity

Secure Intelligent Transportation System

A. Secure communication in V2X network

- Data exchange in the form of Vehicle Record (VR)
- VR relies on Active Bundle (AB) [1], [2], [3] concept and incorporates:
 - encrypted key-value pairs (AES algorithm)
 - access control and metadata policies
 - policy enforcement engine

Example of key-value pair:

`vr.vehicleOwnerName : Enc(John Doe)`

Secure Intelligent Transportation System

A. Secure communication in V2X network

Assumptions:

- 1) Hardware and OS that run VR are trusted
- 2) Https protocol used for communications between the web services

Features:

- Encryption key (AES) is generated on-the-fly based on VR (AB) execution flow [2]
- On-the-fly authorized data updates are supported



Secure Intelligent Transportation System

A. Secure communication in V2X network

VR Example

PrimKey	Owner Info	Vehicle Info	Road Event
ID	Name	License Plate	Accident
	Home Address	VIN	Obstacle
	Drivers License	Health Report	Traffic Jam
	Phone	Engine parameters	Road Work
	Email	Fluid Level	Weather Alert
		Mileage	
		Tire Pressure	
		Performance Report	
		Average Speed	
		Trip Mileage	

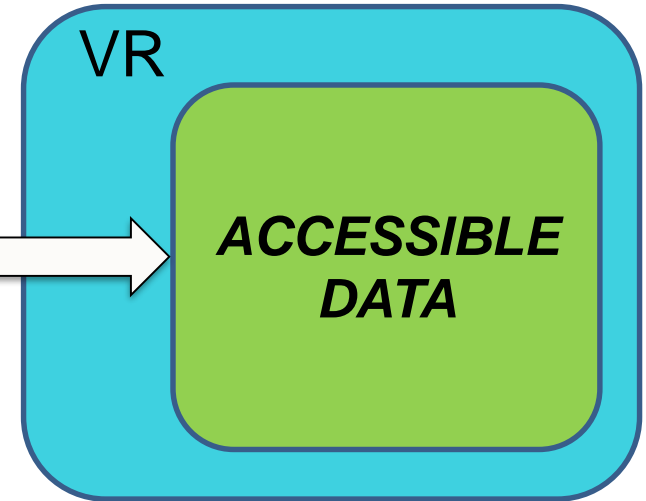
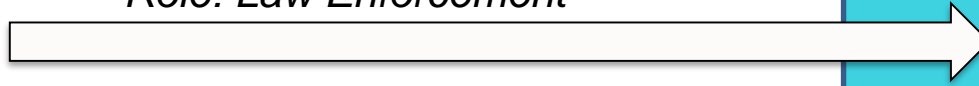
Secure Intelligent Transportation System

A. Secure communication in V2X network



**AUTHENTICATED
CLIENT**

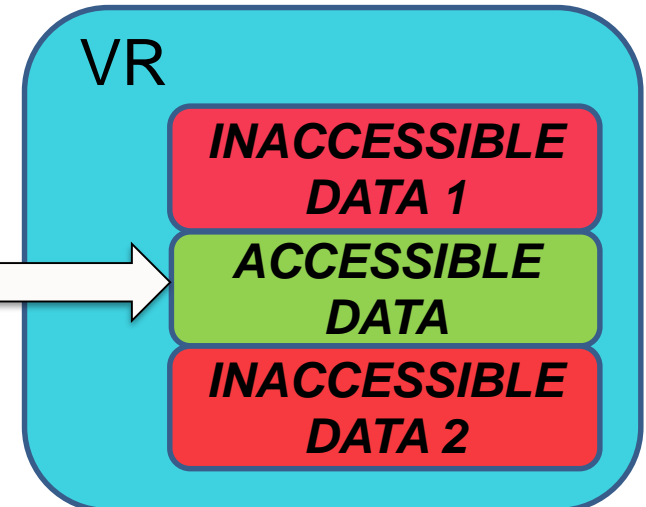
*Browser's Crypto Level: High
Authentication Method: Fingerprint
Client's device: Desktop
Source network: Corporate Intranet
Role: Law Enforcement*



**AUTHENTICATED
CLIENT**



*Browser's Crypto Level: Low
Authentication Method: Password
Client's device: Mobile
Source network: Unknown
Role: Insurance Service*



Secure Intelligent Transportation System

A. Secure communication in V2X network

- Access control policies are specified by data owner: driver and/or vehicle manufacturer
- Example of 4 services in V2X network: Law Enforcement, Car Repair Service, Insurance, Other Drivers

ALLOW

Resource	Driver's License Number	VIN	Owner's Address	Traffic Events
Subject Role	Law Enforcement	Law Enforcement, Car Repair	Law Enforcement, Car Repair, Insurance	Law Enforcement, Insurance, Other Drivers
Action	Read	Read	Read	Read

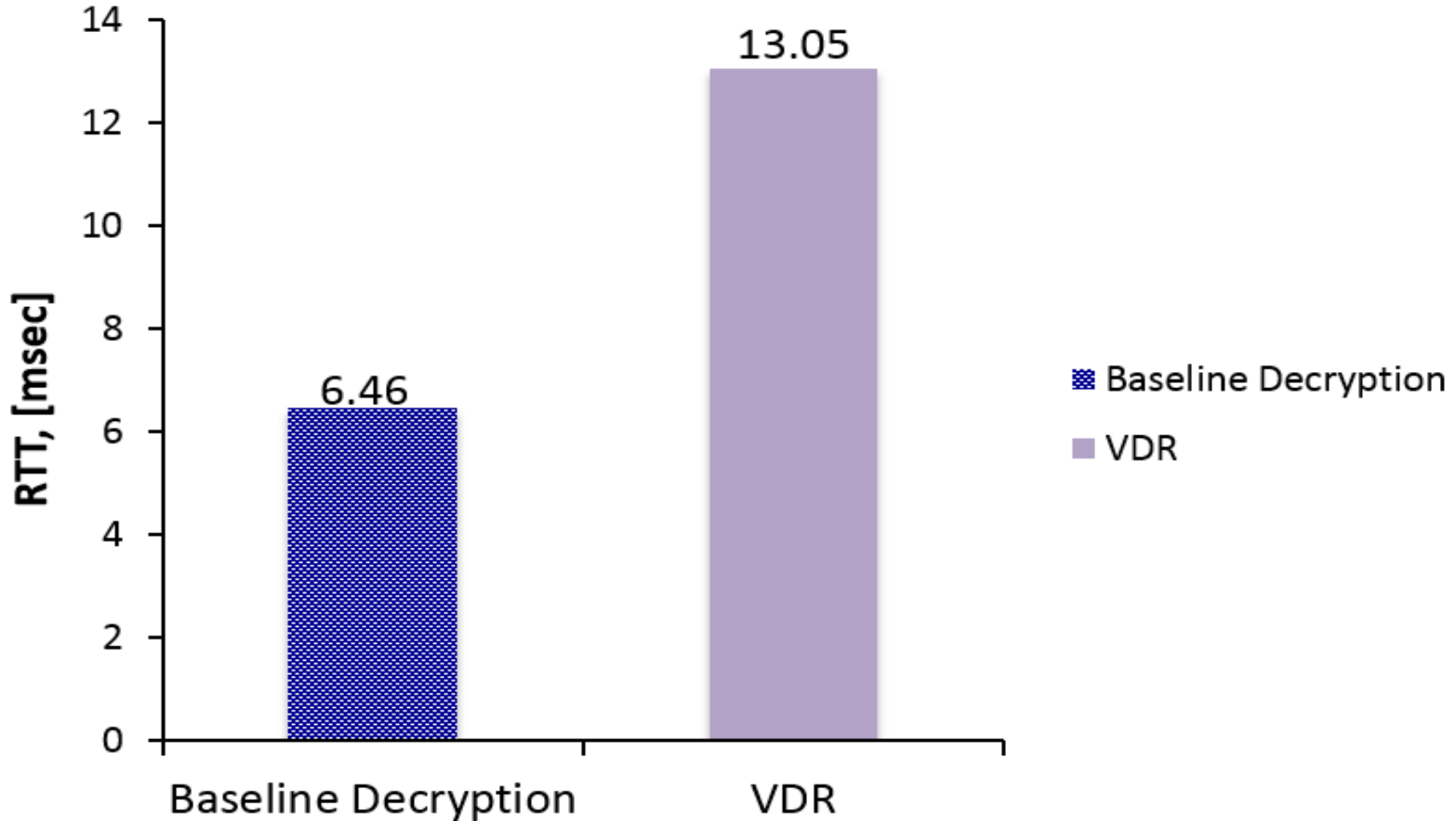
Experiment 1

Input data:

- 617 bytes of data encrypted with AES algorithm
 - in VDR encrypted data is incorporated together with access control policies, policy enforcement engine, providing tamper-resistance, and with data leakage detection engine
 - in baseline, data is just encrypted and there are no access control policies to be evaluated and no identity management
- **Experimental Setup**
 - Client (one vehicle) sends a request to VDR, hosted locally, for 617 bytes dataset
 - In baseline, 617 bytes of data are just decrypted with AES
 - Vehicle is represented as Raspberry Pi Model B with ARMv7 Processor rev 4 @1.2GHz, RAM 1GB, Raspbian GNU/Linux 9.1 (stretch) operating system

Experiment 1

Inter-vehicle data exchange Round-Trip Time



Experiment 1

Output

- Round-trip time between sending a local data request and receiving a result

Conclusion

- VDR imposes 102% overhead, but, compared to baseline, it supports the following:
 - Role-based and attribute-based access control
 - Identity management
 - Tamper-resistance
 - Data leakage detection

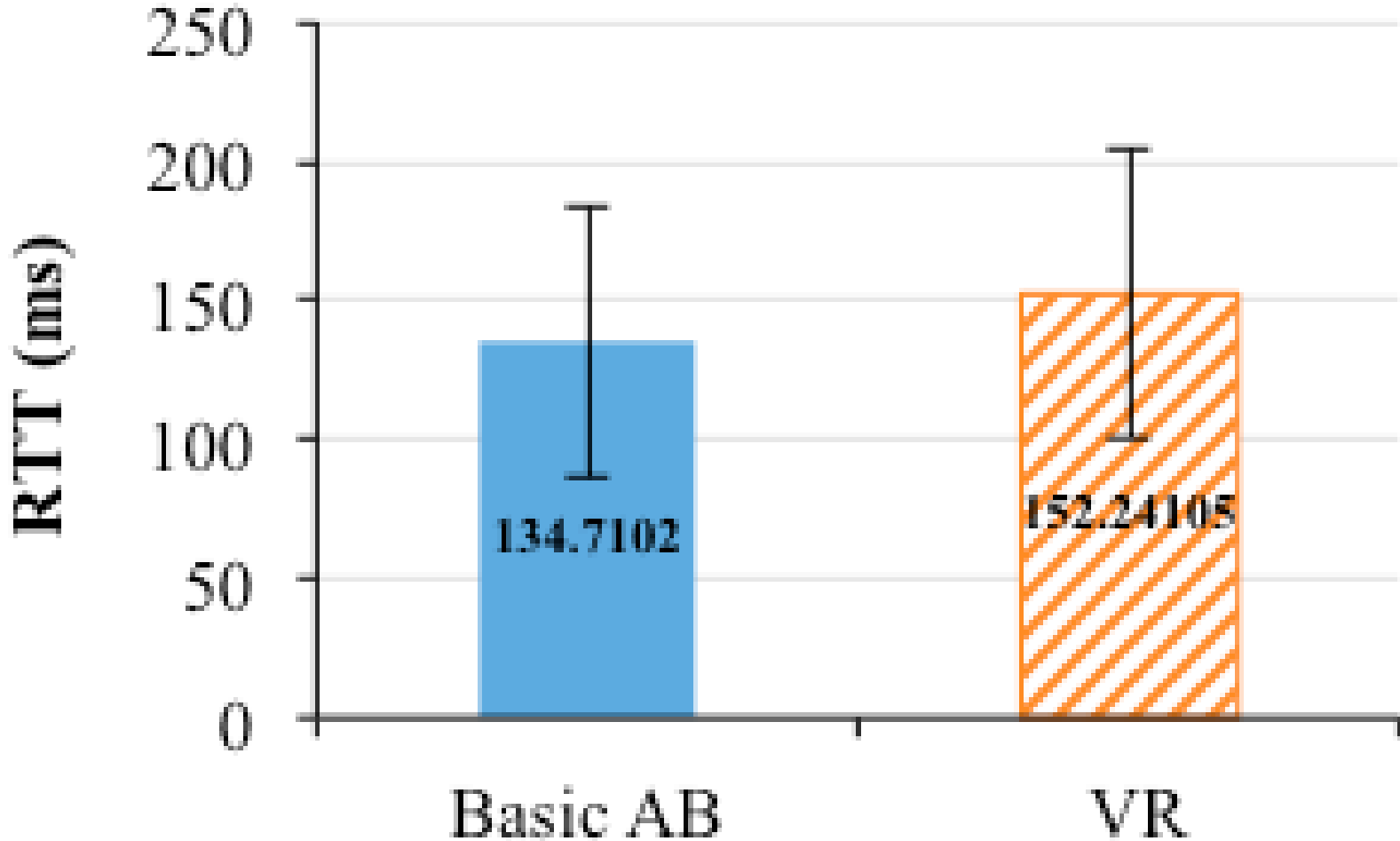
Experiment 2

Input data:

- Basic Active Bundle (AB) and Vehicle Record (VR), containing 617 bytes of selected vehicle data
 - VR, in contrast with AB, provides tamper-resistance, extended attribute-based access control and data leakage detection
- **Experimental Setup**
 - Client (one vehicle) sends an http request over wireless network to another vehicle, hosting VR (or AB), for 617 bytes dataset
 - Each vehicle is represented as Raspberry Pi Model B with ARMv7 Processor rev 4 @1.2GHz, RAM 1GB, Raspbian GNU/Linux 9.1 (stretch) operating system

Experiment 2

Inter-vehicle data exchange Round-Trip Time



Experiment 2

Output

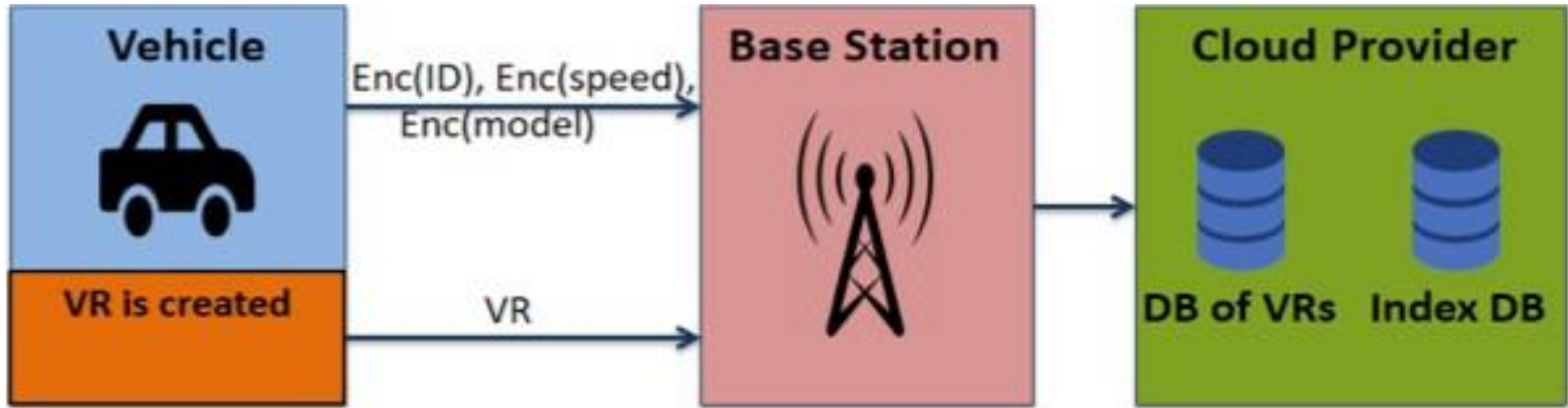
- Round-trip time between sending a data request and receiving a result

Conclusion

- VR imposes 13% overhead, but, compared to AB, supports the following:
 - Extended attribute-based access control
 - Tamper-resistance
 - Data leakage detection
- Wireless network delays impact the results

Secure Intelligent Transportation System

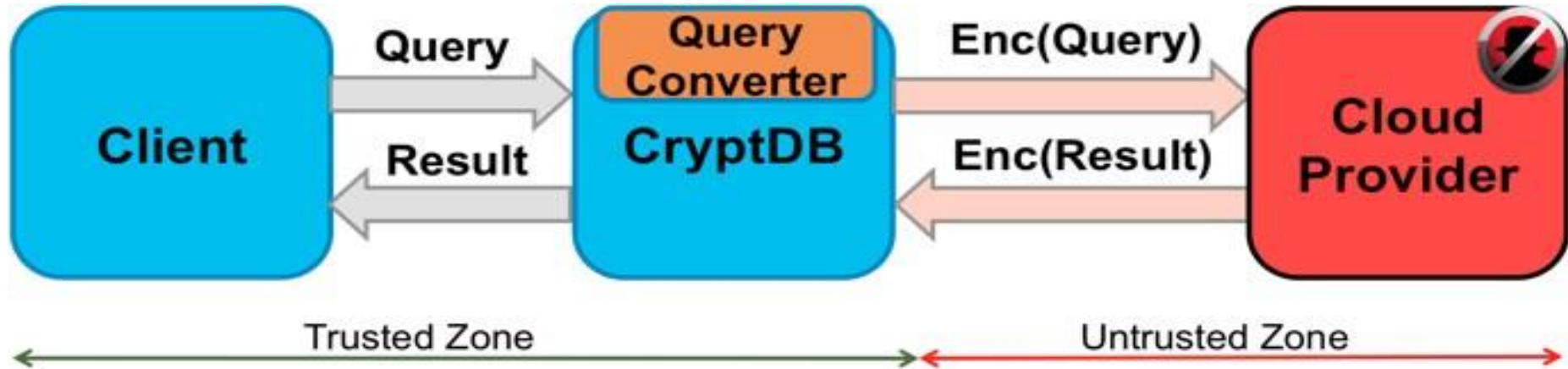
B. Encrypted Search over Encrypted Records



- VR is created on a vehicle and is sent to Cloud Provider
- Cloud Provider stores database of VRs and auxiliary Index Database used to build index to speed up SQL queries execution
- Data query first phase: find relevant VRs in Index DB by their IDs
- Data query second phase: query relevant VRs in DB of VRs for a particular attribute, e.g. vehicle owner's home address

Secure Intelligent Transportation System

B. Encrypted Search over Encrypted Records



- Use case 1: law enforcement needs personal data of drivers who exceeded speed limit of 65 mph and went above 76 mph
- Initial Query: `SELECT ID FROM IndexDB WHERE SPEED > 76`
- Converted query: `SELECT c1 FROM Alias1
WHERE ESRCH (Enc (Speed) , Enc (76)) ;`
- Second phase query: http get request for driver's license number from VRs with relevant IDs from previous query

Secure Intelligent Transportation System

B. Encrypted Search over Encrypted Records

=>

Index Database

Use case 2: ITS

needs to figure out the traffic pattern during rush hour.

Speed between 55

and 65 means no traffic jam

ID	Speed	Model	Timestamp
<u>Enc(001)</u>	<u>Enc(65)</u>	<u>Enc(Toyota)</u>	02/18/2018 15:28
<u>Enc(002)</u>	<u>Enc(66)</u>	<u>Enc(Ford)</u>	02/18/2018 15:29
<u>Enc(003)</u>	<u>Enc(67)</u>	<u>Enc(Mercedes)</u>	02/18/2018 15:31
<u>Enc(004)</u>	<u>Enc(68)</u>	<u>Enc(Mitsubishi)</u>	02/18/2018 15:44
⋮	⋮	⋮	⋮
<u>Enc(1000)</u>	<u>Enc(84)</u>	<u>Enc(Chevrolet)</u>	02/18/2018 23:59

- Initial Query: `select ID from IndexDB WHERE speed between 55 and 65`
- Converted query: `SELECT c1 FROM Alias1 WHERE ERANGE (Enc (Speed), Enc (55), Enc (65) ;`
- Second phase query: http get request for vehicle's license plate number from VRs with relevant IDs from previous query

Secure Intelligent Transportation System

B. Encrypted Search over Encrypted Records

Operations supported by different encryption schemes

Encryption Scheme	Homomorphic Property	Supported Operations	Example
<u>Paillier</u>	AHE	+, SUM	Count sum of tolls paid by vehicles on a highway
<u>ElGamal</u>	MHE	*	Count covered distance which is multiplication: time * average speed
<u>Boldyreva et al.</u>	OPE	<, >, MIN, MAX	select ID, Speed, Model from <u>IndexDB</u> where Speed between 71 and 80
SWP	SRCH	Tokenized search	select Model from <u>IndexDB</u> where issue LIKE %battery%
AES	DET	Exact search	select ID, Speed from <u>IndexDB</u> where Model = 'Ford'

Experiment 3

Input data:

- Regular MySQL database with 1000 tuples
- CryptDB encrypted database with same 1000 tuples
- **Experimental Setup**
 - Databases are hosted by a server 1.9GHz CPU and 1GB RAM, with Linux Ubuntu 12.04.5 LTS (kernel 3.13.0-32-generic, 64-bit)
 - 5 SQL Queries run against MySQL and CryptDB databases with the same data (same 1000 tuples)

Experiment 3

- **Experimental Setup**

- SQL Queries:

- Equality query (Q1): **SELECT ID FROM IndexDB
WHERE model = Ford**

- Inequality query (Q2):

- SELECT ID, speed, model FROM IndexDB WHERE speed > 80**

- Inequality query, shortened (Q3):

- SELECT ID FROM IndexDB WHERE speed > 80**

- Range query (Q4):

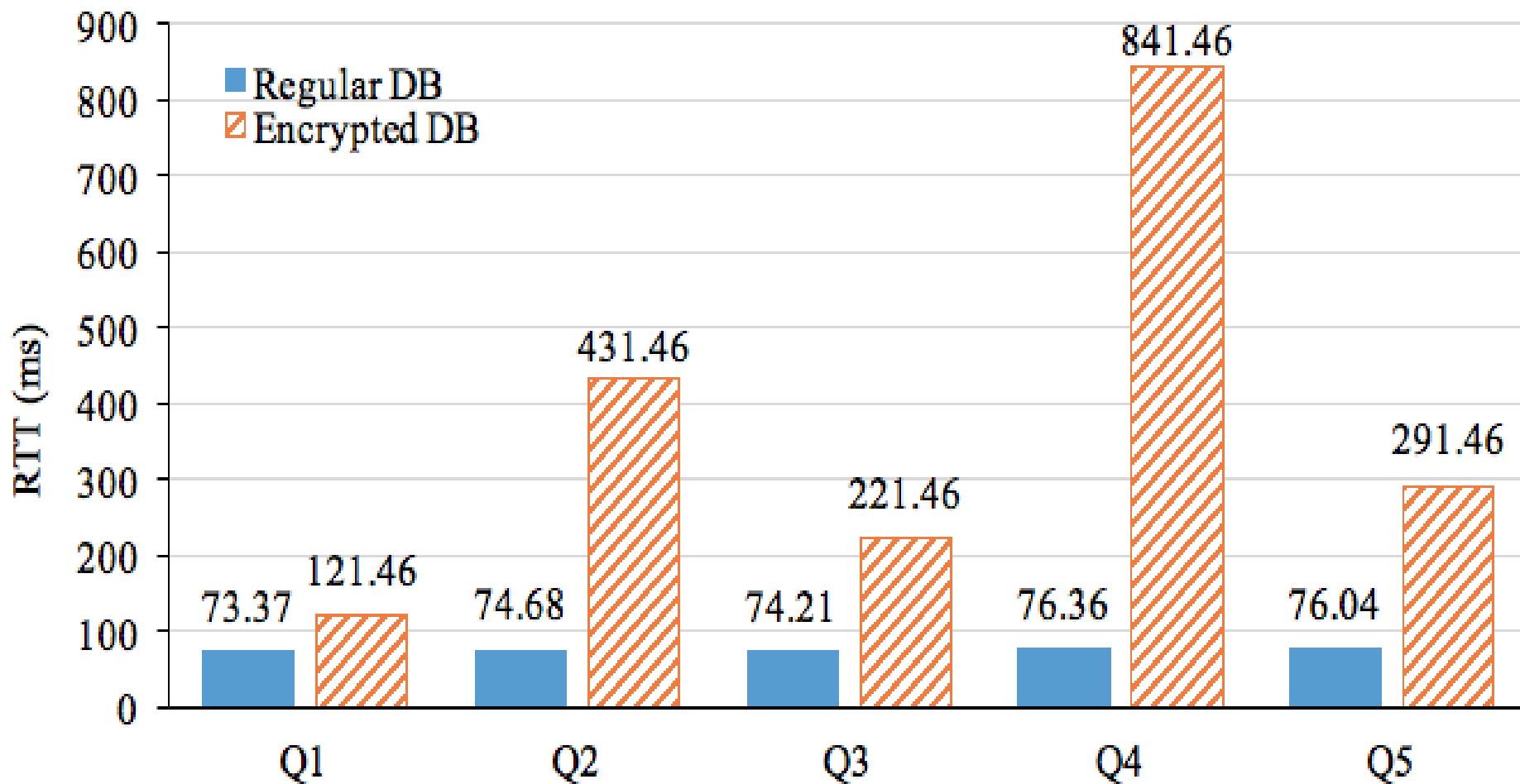
- SELECT ID, speed, model FROM IndexDB
WHERE speed BETWEEN 71 AND 80**

- Range query, shortened (Q5):

- SELECT ID FROM IndexDB WHERE speed BETWEEN 71
AND 80**

Experiment 3

SQL Query execution time on regular and encrypted database



Experiment 3

Output

- SQL Query execution time on regular and encrypted database

Conclusion

- SQL Query execution times increases in CryptDB compared to plaintext MySQL database by:
 - 26 times for Q1
 - 112 times for Q2 (all 3 obtained attributes need to be decrypted)
 - 54 times for Q3 (only ID needs to be decrypted)
 - 157 times for Q4
 - 48 times for Q5

Secure Intelligent Transportation System

C. Vehicle Recognition

- We utilize **Sighthound** by Dehghan et al. [8]: a vehicle make, model, and color recognition (MMCR) system
- **Sighthound** relies on a deep convolutional neural network
- We wrapped **Sighthound JavaScript API** [14] to retrieve results from the classifier
- Vehicle Make, Model and Color are used to derive decryption key for “Summary” field of Vehicle Record (see section D “Decentralized Machine Learning Analytics”)
- “Summary” field is used to build analytics over encrypted Vehicle Records

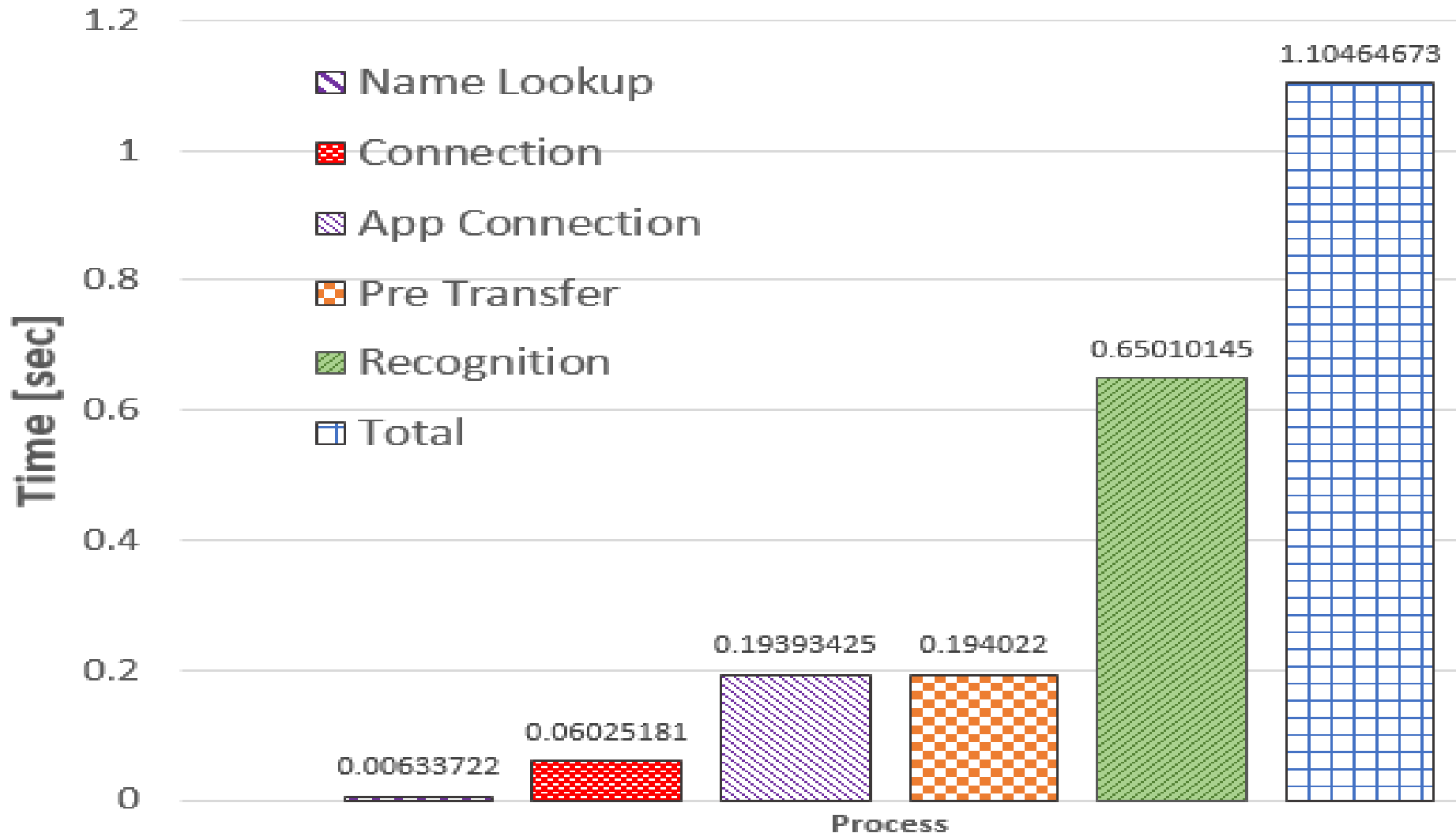
Experiment 4

Input data:

- A hundred different pictures taken from the **Car Dataset [21]**
- **Experimental Setup**
 - We craft multiple (i.e., a hundred) requests to the cloud provider (i.e., **Sighthound RESTful API [14]**).
 - Single-machine experiments were run using a machine with Intel Core i7 (4 cores @2.8GHz, 8MiB cache) with 16GiB of RAM.
 - The goal is to simulate a real scenario in which we query the cloud (the cloud will contain our trained model) and return the results to the certifying authority (e.g., toll booth station).

Experiment 4

Vehicle recognition at a toll booth using cloud



Experiment 4

Output

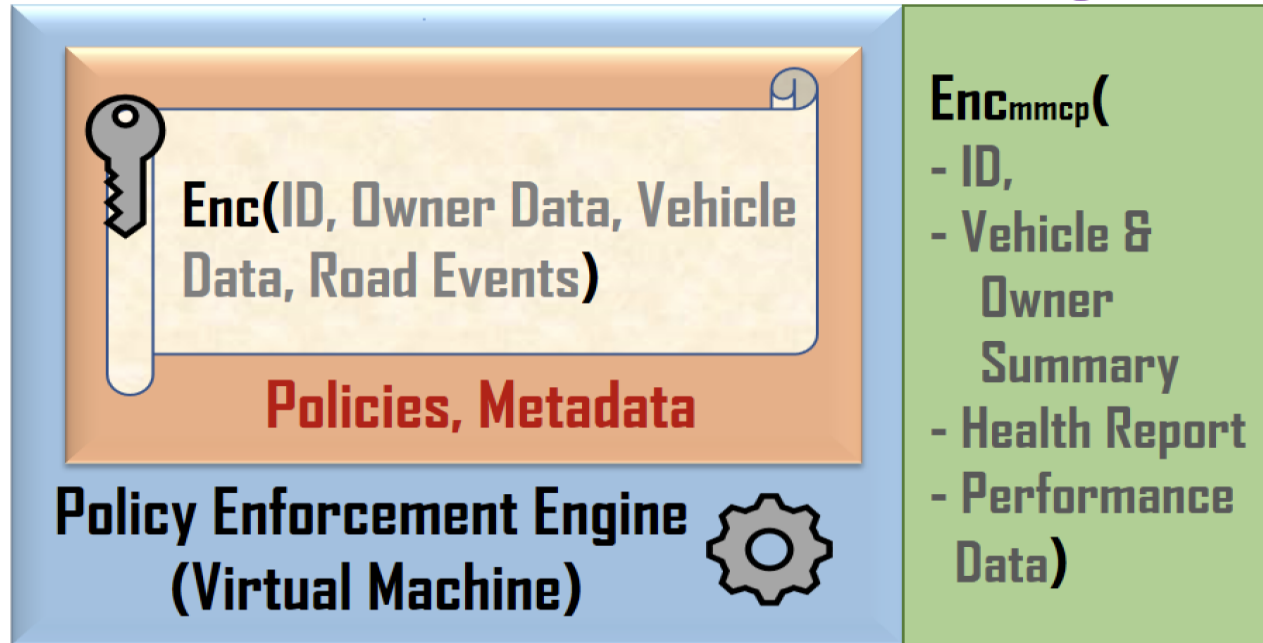
- Total running time for the **MMCR** algorithm. This measurement includes image transmission, connection, algorithm running time and name lookup.

Conclusion

- Our experimental results demonstrate the feasibility of our idea (**the total processing time per request is around one second**).

Secure Intelligent Transportation System

D. Decentralized Machine Learning Analytics



- Vehicle Data Record (VDR) has a “summary” field that can be accessed bypassing access control policies evaluation
- “Summary” field is encrypted with MMCR key, derived based on vehicle’s make, model and color (see section C)

Secure Intelligent Transportation System

D. Decentralized Machine Learning Analytics

- Provenance data, stored in VDR, is used for aggregated analytics such as *Count*, *Average*, *etc.* on qualified attributes in individual vehicles on-the-fly.
- These aggregate analytics guarantee privacy of individual vehicles and help in decision making.
- Consider an aggregation,
 - VDR₁'s attribute A is perturbed: “A” + “Random Perturbation (R)” → VDR₁(A + R = A_n) + VDR₂(A + A_n = A_{n1}) + ...
 - Final average = (A_{nn} - R) / count(VDR)

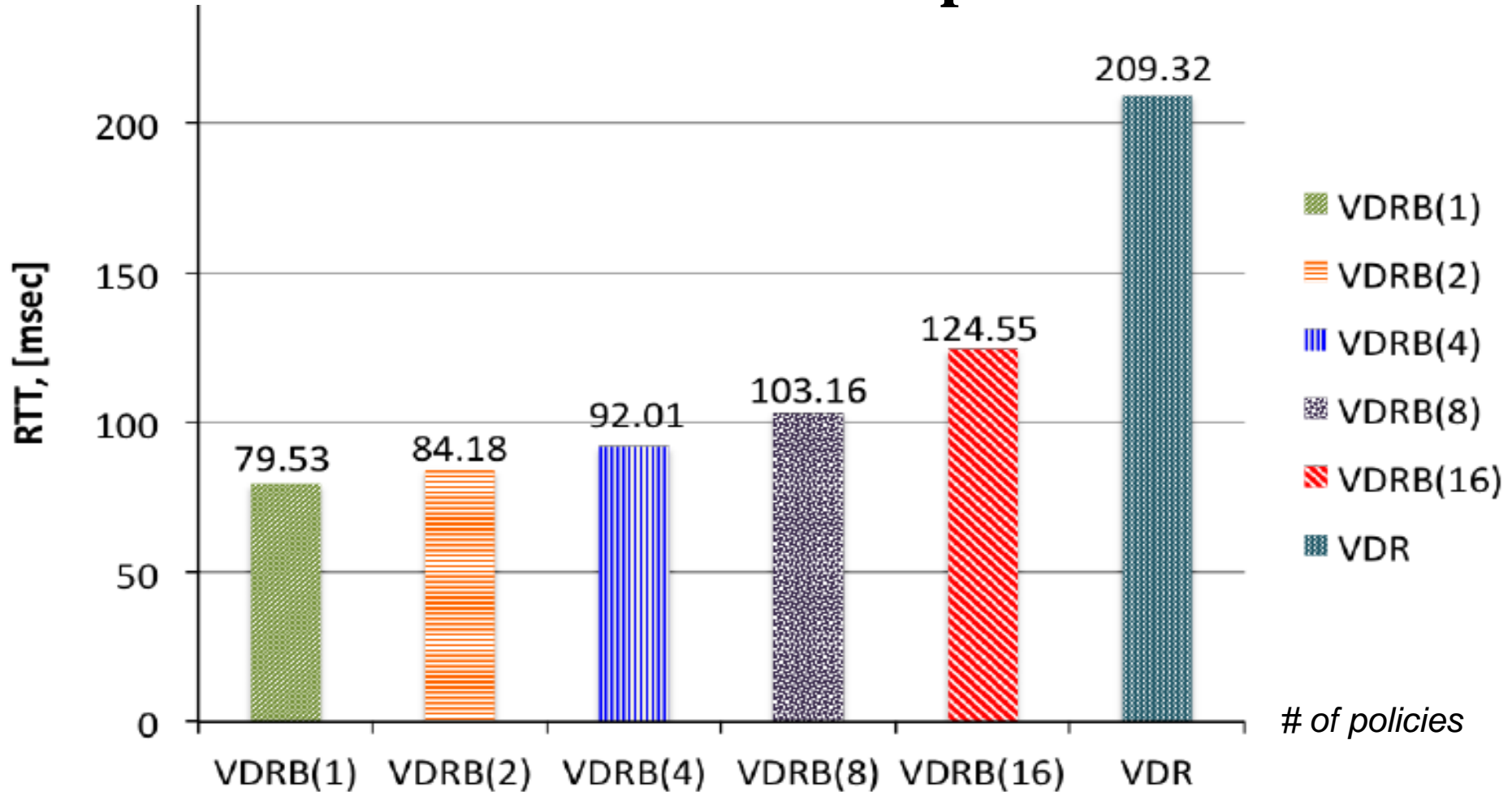
Experiment 5

Input data:

- VDR baseline (VDRB) with different number of access control policies: 1, 2, 4, 8, 16
- VDR, in contrast with VDRB, provides tamper-resistance, extended attribute-based access control, on-the-fly data analytics and data leakage detection
- **Experimental Setup**
 - Client (one vehicle) sends a request to another vehicle, hosting VDR or VDRB, for 617 bytes dataset over wireless network
 - Vehicle is represented as a Raspberry Pi Model B with ARMv7 Processor rev 4 @1.2GHz, RAM 1GB, Raspbian GNU/Linux 9.1 (stretch) operating system

Experiment 5

VDR Round-Trip Time between two vehicles for various number of access control policies



Experiment 5

Output

- Round-trip time between sending a remote data request to vehicle, hosting VDR(B), and receiving result

Conclusion

- VDR with 4 access control policies imposes 127% overhead, but, compared to VDRB, it supports the following:
 - Extended attribute-based access control
 - Tamper-resistance
 - Data leakage detection
 - Fast on-the-fly decentralized data analytics
- Wireless network delays impact results

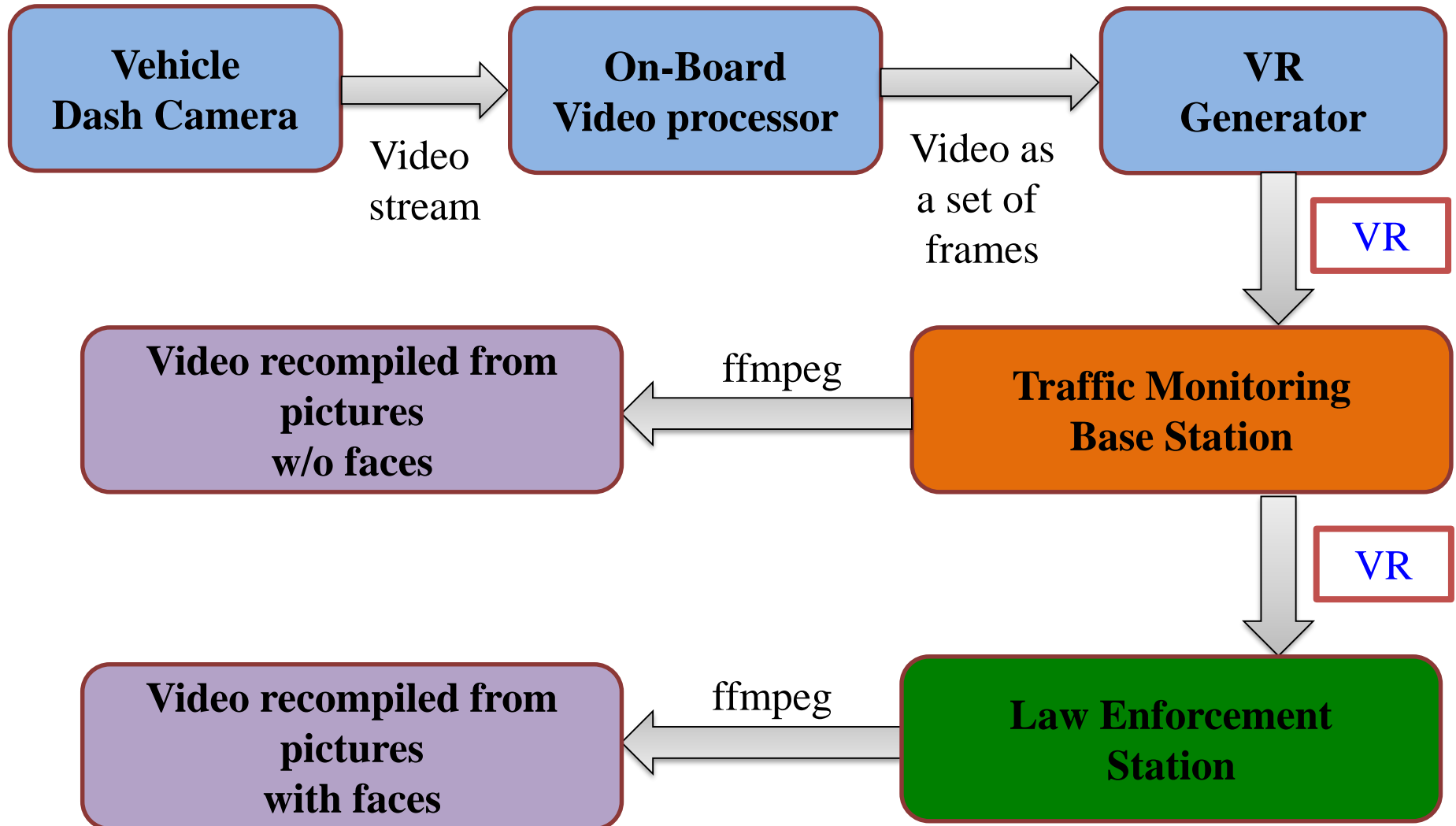
Secure Intelligent Transportation System

E. Secure Video Transfer and Face Detection

- Dashed camera captures the video
- Face detection algorithms (from “**OpenCV**” [7] library) are applied to each frame of video
- Face detection result is used in access control policies
 - Video fragments with human faces are accessible only by Law Enforcement entity, but not by other vehicles drivers
 - Video fragments without human faces are accessible by other vehicles drivers [5]
 - “**ffmpeg**” utility is used to recompile videos from the set of frames

Secure Intelligent Transportation System

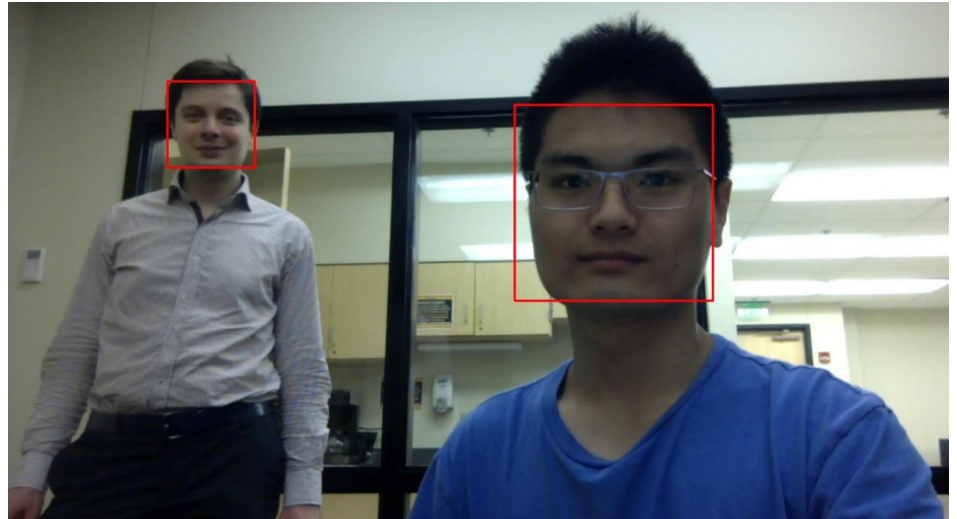
E. Secure Video Transfer and Face Detection



Secure Intelligent Transportation System

E. Secure Video Transfer and Face Detection

- 4 face detection algorithms (cascade classifiers) from OpenCV [7] library:
 - haarcascade_frontalface_alt
 - haarcascade_frontalface_alt2
 - haarcascade_frontalface_default
 - lbpcascade_frontalface



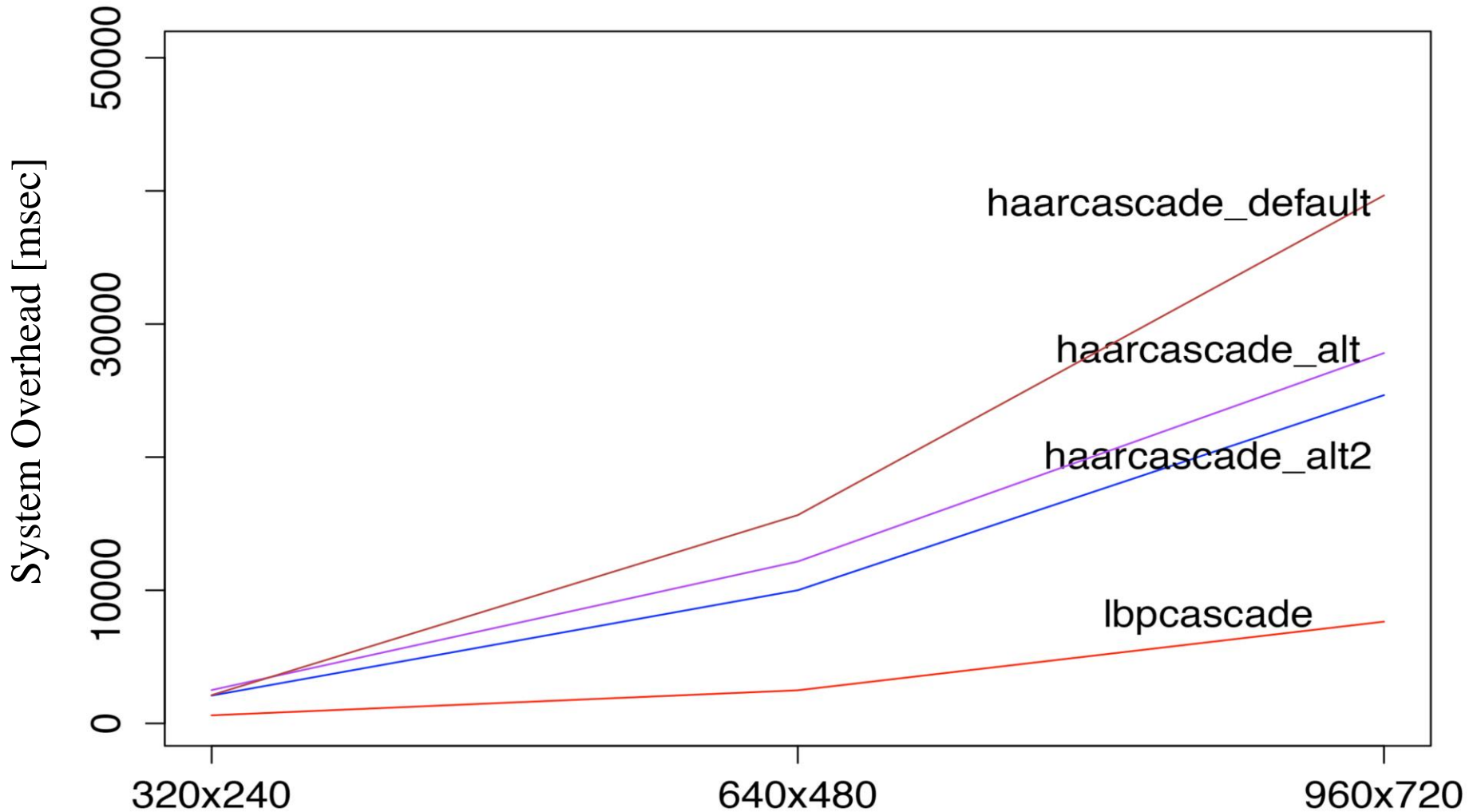
Experiment 6

Input data:

- Images with three different resolutions: 320x240, 640x480, 960x720 pixels
- **Experimental Setup**
 - 4 different face detection algorithms (from OpenCV library) are applied to images with 3 different resolution
 - Hardware platform: Raspberry Pi Model B with ARMv7 Processor rev 4 @1.2GHz, RAM 1GB, Raspbian GNU/Linux 9.1 (stretch) operating system

Experiment 6

Face detection algorithms performance



Experiment 6

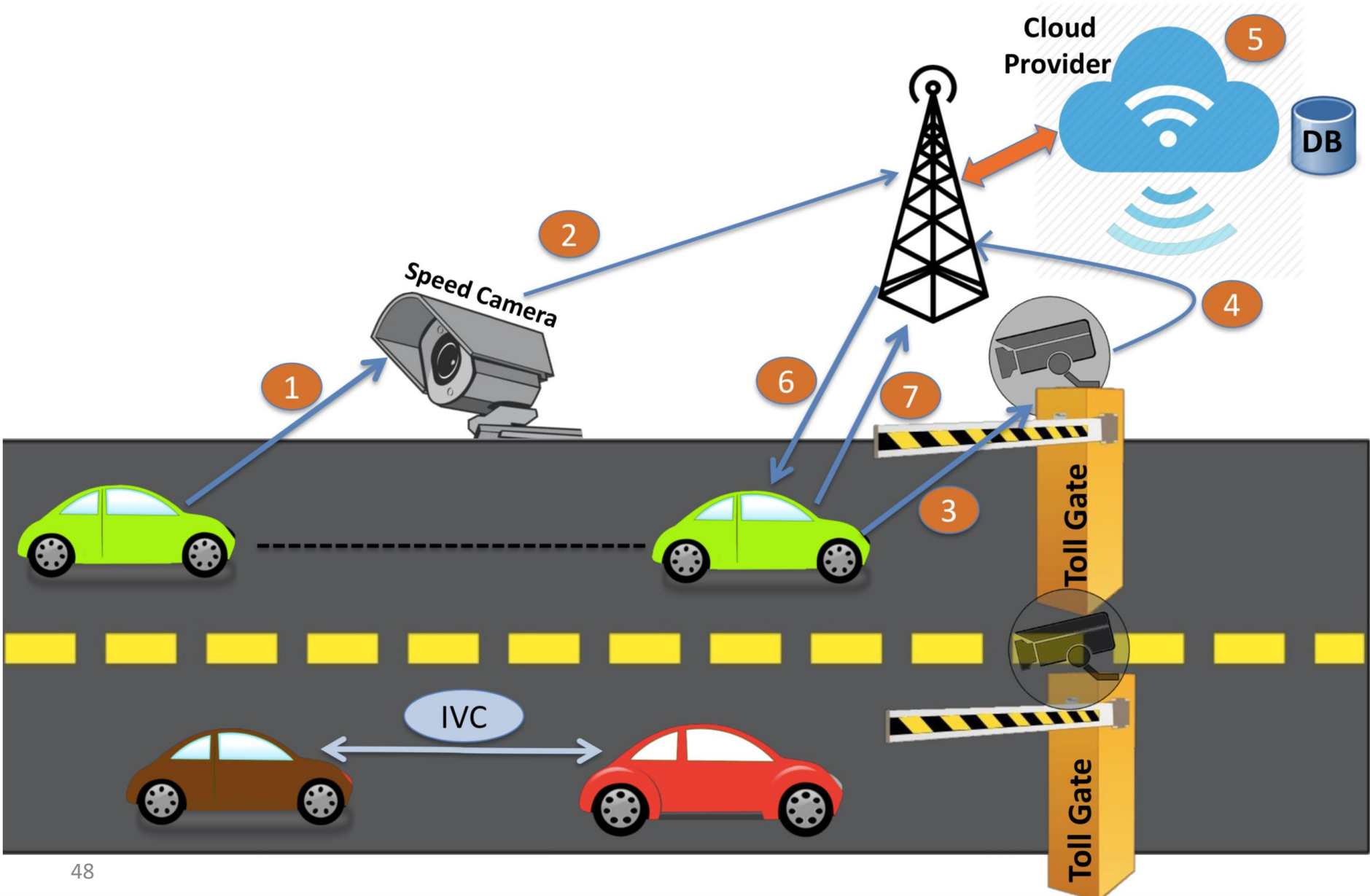
Output

- Image processing time till giving a face detection result YES/NO

Conclusion

- “**Haar Cascade Alternative 2**” is the best algorithm: has the highest detection rate (73%) with the second lowest overhead [22]
- Images with greater resolution take longer to be processed

System Architecture



System Architecture

Step 1. Speed camera captures vehicle speed and license plate and sends them together with the speed limit at step 2 to cloud provider

Step 3. Once vehicle reaches the toll gate, the high-resolution camera captures make, model, color, license plate number and sends them at *step 4* to cloud provider, where they are used to derive a unique encryption MMCP key at *step 5*

Step 6. MMCP encryption key is sent to vehicle, along with previously captured at steps 1, 2 pairs of (speed, speed limit)

Step 7. all the vehicles attributes are bonded together and Vehicle Data Record (VDR) is created, having them in encrypted form

- VDR is created locally at the vehicle to guarantee protection against malicious or curious cloud administrators.

Security vs. Safety

FOCUS:

- How much the use of secure communication affects safety
- Systematic attack analysis [20]



Complexity of authentication mechanisms:

Complexity \uparrow \rightarrow Security \uparrow \rightarrow Performance \downarrow

Key management:

PKI: Key management time \downarrow , authentication time \uparrow

Symmetric : Key management time \uparrow , authentication time \downarrow

Certificate revocation:

Performance \uparrow \rightarrow Safety \uparrow , Security \uparrow

Privacy:

Complexity \uparrow \rightarrow Security \uparrow \rightarrow Performance \downarrow


Security vs. Safety

Attacks

- Replay Attack
- GPS Spoofing
- Tunneling
- Position Faking
- Message Tampering
- Message Suppression/Fabrication/Alteration
- Sybil Attack
- DoS Attack
- Black Hole Attack
- Broadcast Tampering
- Eavesdropping
- Stealing Location Information

Security vs. Safety

Categories of Safety messages in V2X network

- **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

Security vs. Safety

Methodology to evaluate Security vs. Safety

- Security overhead when there is no attack
- Security overhead when there is an attack
- Safety level when there is no attack
- Safety level when there is an attack but no security mechanism provided
- Safety level when there is an attack and security mechanism is provided

Security vs. Safety

Performance Metrics [20]

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

Security vs. Safety

Systematic Attack Analysis [20]

Anatomy of an Attack: step-by-step breakdown of the features (or actions) that occur when an attack is deployed on a vehicle

Name: Each attack is identified by a unique identifier. *ATTACK* followed by a number represents the code of the attack or the mitigation mechanism. Following the code is the name of the attack or the mechanism being analyzed in the unit

Description: Description defines an attack or a mechanism being analyzed. The description provides a brief overview of the pursuit of the attack

Security vs. Safety

Systematic Attack Analysis

Features: consist of the transactions that form an attack. T represents transactions. $T00$ corresponds to the initial step taken by the target. $T0$ transactions correspond to regular operations of the target component. T followed by any other number is a unique code for a transaction or feature. State of the target (connected ($T01a$) or disconnected ($T01b$)) is assumed to be connected at the beginning

Mitigation: Each attack can be prevented by a corresponding mitigation mechanism. For a given mitigation, there is a cost associated with its deployment.

Security vs. Safety

Systematic Attack Analysis

Cost: Each attack has some associated cost. That is, there is a cost associated with implementing the attack as well as the impact that it has after it has been implemented. The same also applies for each mitigation, where it has cost associated with its deployments.

Impact on safety: it defines how utilizing a mitigation mechanism influences the system's safety

Impact on security: it defines how utilizing a mitigation mechanism influences the security of the system

Security vs. Safety

Example of Systematic Attack Analysis [20]

Code	Transaction	Response(s)	Time	Other Overhead	Total Cost
T00	Receive message	insert message into queue Transmission rate	5 ms (time to wait in the queue) T_x	100-200 Bytes message size + 256 bytes (size of the key) influence the number of message received or sent storage of messages	5 ms T_x
T1	Message Authentication	verify content relevancy generate signature verify signature	0.05ms (identify critical keys in the message such as accident, traffic, etc.) 0.171 ms (assumption) 5 ms (assumption)		5. 221 ms
T2	Collision Distance	read and update location compute proximity to preceding vehicle or car aside update status	5 ms 0.5 ms		5.5 ms
T3	Notification	send notification if distance below threshold	2 ms (transmission time between sensor and notification system)		2ms
Total overhead					17 - 20 ms + T_x

Security vs. Safety

Example of Systematic Attack Analysis

Mitigation:

- Firewall to filter-out packets arriving to vehicular network to prevent network flooding
- Timestamp can be used to assess if the timestamp on the message has not been modified

Costs:

- Cost of the attack
 - C1: Warning/alert is not received in a timely manner for usefulness
 - C2: Response delay
 - C3: Entering dangerous road situation such as collision or causing traffic jam
- Cost of mitigation: Computation overhead increases system reaction time

Security vs. Safety

Example of Systematic Attack Analysis

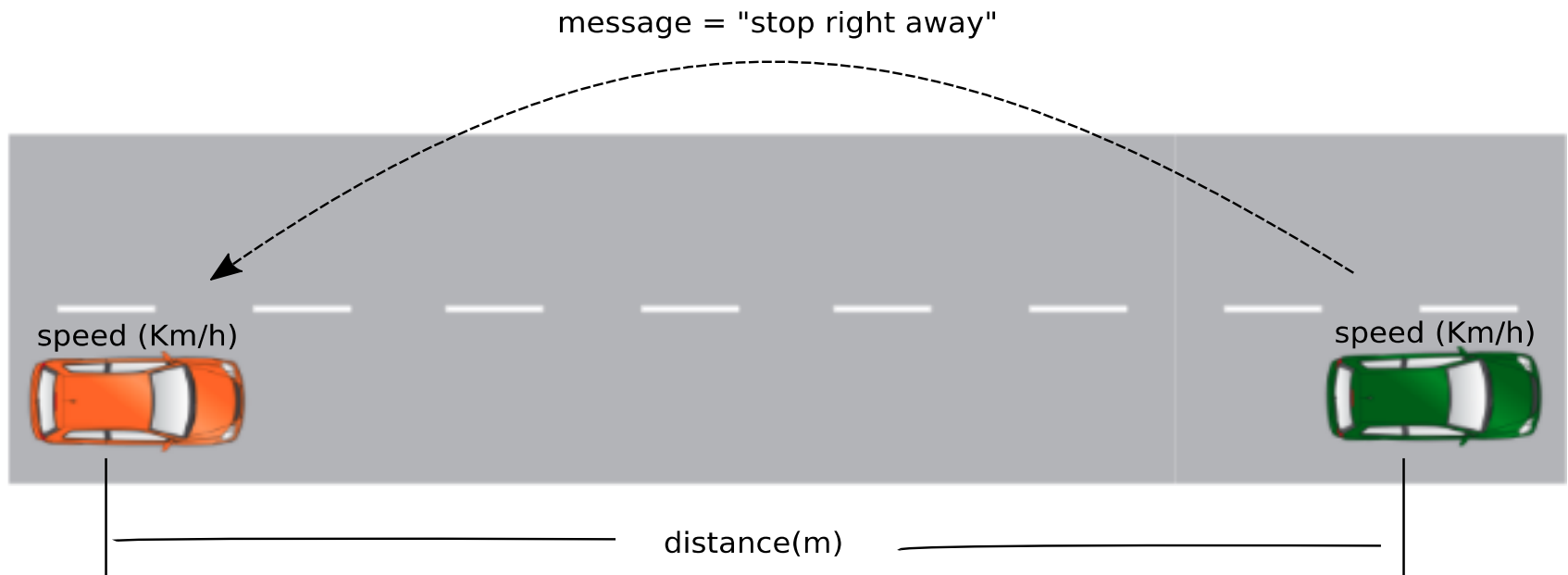
Impact on Safety: checking of arriving packets by a firewall in order to filter-out malicious data packets may result in messages from other vehicles or roadside units (RSU) failing to reach the destination in time. E.g. if a message about a collision or an obstacle in front of the current vehicle is not received in time, the vehicle could potentially be a subject to a collision

Impact on Security: Since malicious data is filtered out, a firewall prevents an attacker to introduce harm into the vehicle. However, the level of security of the algorithm used imposes high computational overhead

Security vs. Safety

Driving Scenario: sudden stop on a highway [20]

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



Security vs. Safety

Driving Scenario: sudden stop on a highway

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

Security vs. Safety

System Model

- Network:
 - ✓ IEEE 802.11p 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

Security vs. Safety

System Model [20]

- **Security costs for V2V communication:**

- ✓ Processing cost

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

- ✓ Communication cost:

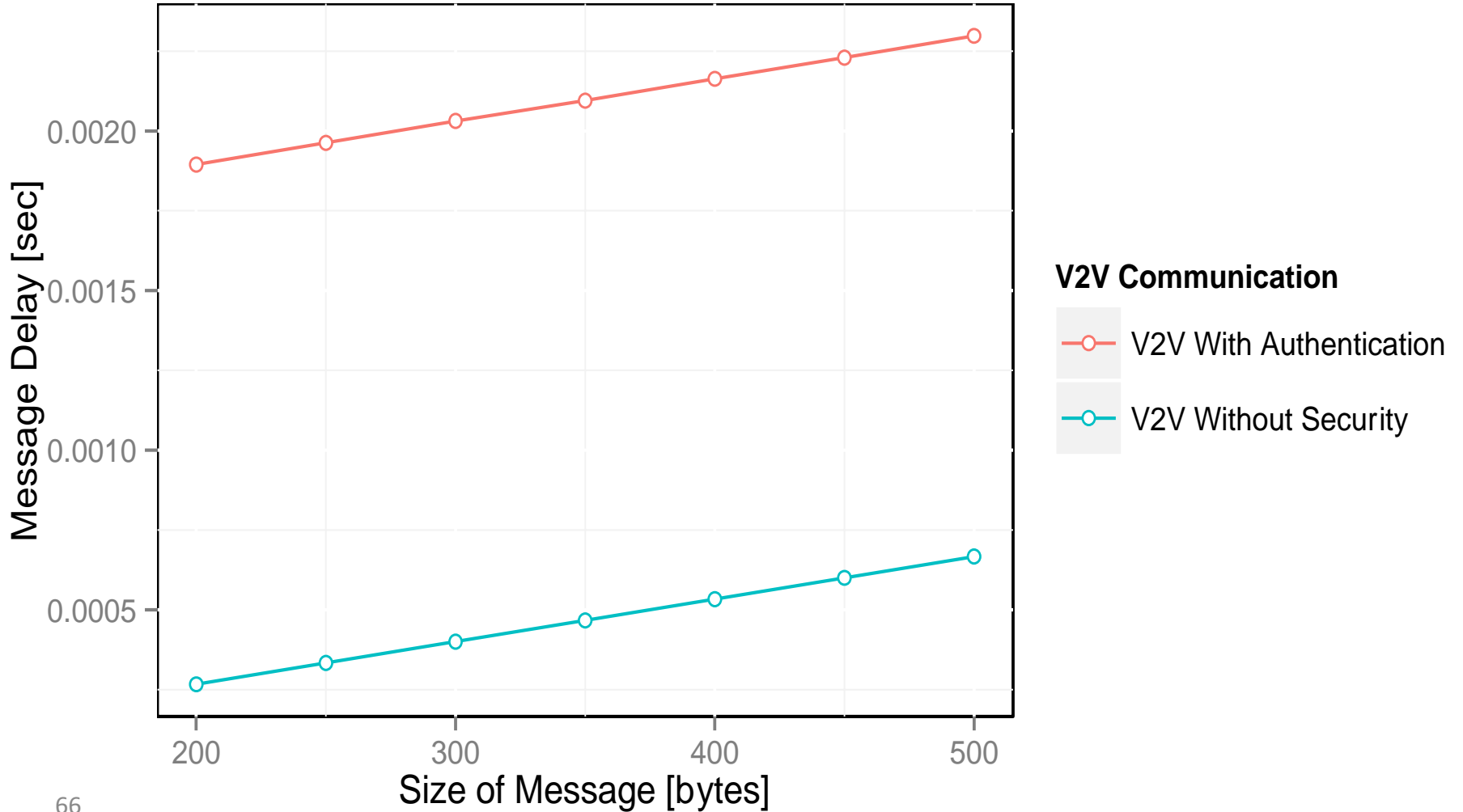
- Distance: 120m
- Bandwidth: 6Mbps
- Speed of communication link: 3×10^8 m/s

Experiment 7

- **Input data:**
 - Two vehicles, Speed: 120Km/h, Distance: 120m
- **Output Data:**
 - Delivery delay for V2V messages with and w/o security mechanisms, [sec]
- **Conclusions:**
 - Delivery delay for V2V messages with embedded security mechanism is about 4 times greater than for V2V messages without security mechanisms
 - Delivery delay for V2V messages grows linearly with the size of message

Experiment 7

Delays for V2V messages delivery with and w/o security

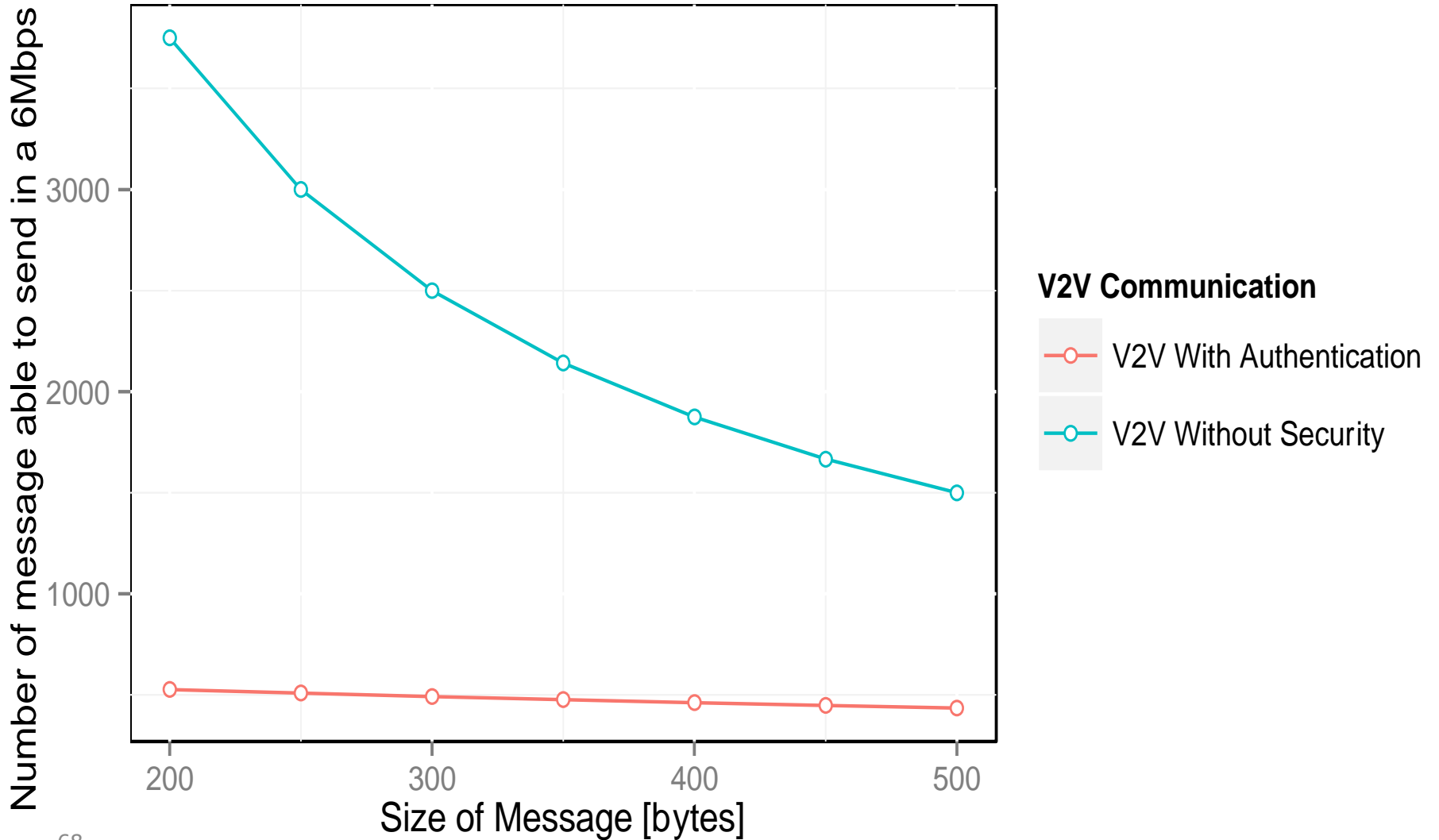


Experiment 8

- **Input data:**
 - Two vehicles, Speed: 120Km/h, Distance: 120m
- **Output Data:**
 - Capacity of V2V communication link, [Mbps]
- **Conclusions:**
 - Capacity of V2V communication link is up to 10 times greater if messages are sent without using secure mechanisms
 - Capacity of V2V communication link for messages sent with authentication slowly drops linearly with size of message
 - Capacity of V2V communication link for messages sent without security mechanism drops exponentially with size of message

Experiment 8

Capacity of V2V communication link, [Mbps]

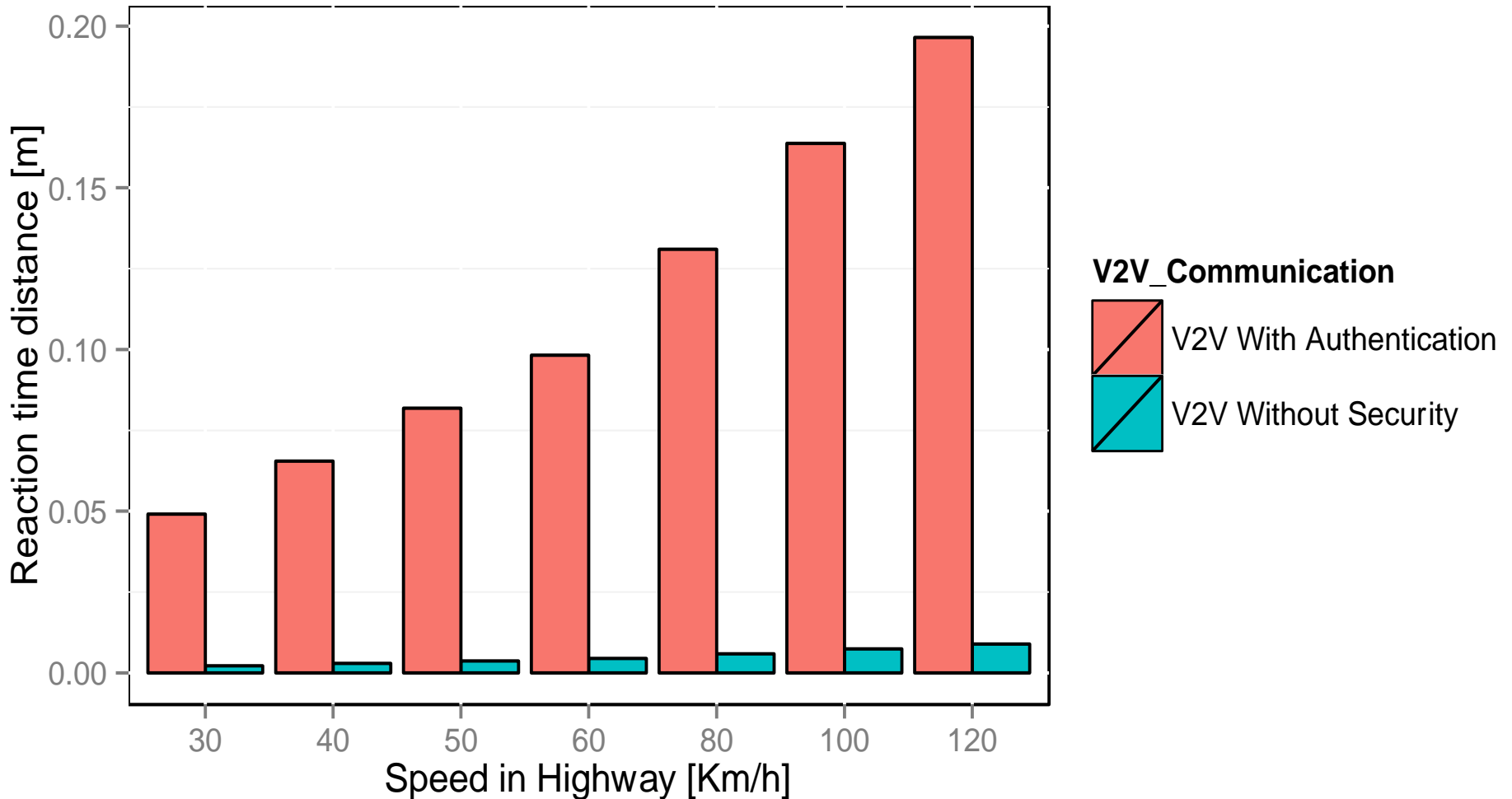


Experiment 9

- **Input data:**
 - 2 vehicles, Distance: 120m, Message size: 200 bytes
- **Output Data:**
 - Reaction time distance in V2V communication system, [m]
- **Conclusions:**
 - Reaction time distance grows linearly with speed
 - Reaction time distance is about 16 times greater for V2V messages with authentication compared to messages sent without any security mechanisms
 - Reaction time distance at speed 120 km/h is about 0.2 [sec] for V2V messages with authentication

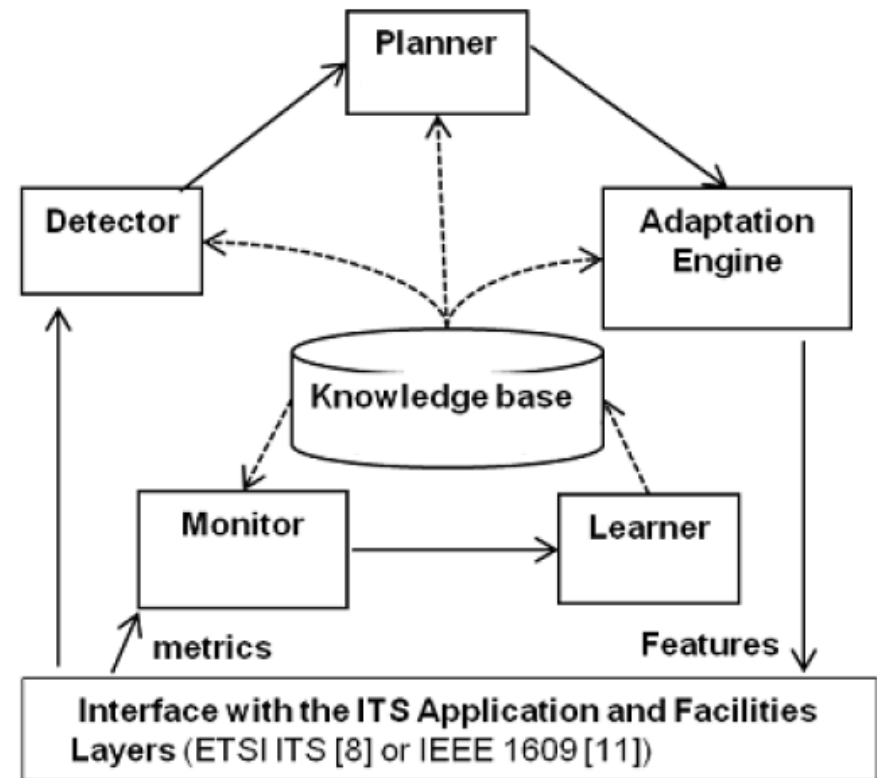
Experiment 9

Reaction time distance, [m] in V2V communication system



Adaptive ITS Design

- Adaptive ITS framework will monitor system behavior and collect performance metrics
- Learn impact of adaptation on the system using machine learning techniques and update the knowledge base
- Detect violations of software requirements
- Plan adaptation to optimize the goals
- Adapt the system at runtime according to the plan



Efficient Monitoring

- V2V software adaptation relies on monitoring the behavior of software
- Typical performance and security metrics include: number of incoming/outgoing packets per second, number of signature generations/verifications per second, packet delays, transmission delays, number of neighboring vehicles/RSUs, quality of radio links etc.
- Monitors can interfere with ITS applications, because they share the same resources (e.g. CPU, memory etc.)
- We need to isolate the monitoring activity from the ITS application

AOP-based Monitoring

- Use aspect-oriented programming (AOP) to monitor behavior of ITS software
- Since all V2V messages do not have the same level of sensitivity to security and privacy, we should use an adaptive security model for V2V, which changes configuration parameters of the secure channel dynamically
- Monitoring and enforcement of the safety and security requirements are achieved seamlessly using AOP

AOP-based Monitoring (cont.)

- AOP is a programming technique allowing for the augmentation of software with cross-cutting concerns, i.e. behaviors that span multiple, often unrelated implementation modules
- AOP enables programmers to cleanly separate aspects and software components, so that cross-cutting concerns of a program can be seamlessly integrated into program code, obviating the need to inline the code for the concern in multiple places.

AOP example for tamper detection

- Example in AspectJ AOP to check the integrity of the code for each method in a Java class named “Authentication” and report existence of tampering if the integrity check fails.
- As clearly seen, the process of adding this monitoring is completely transparent to the actual application code.

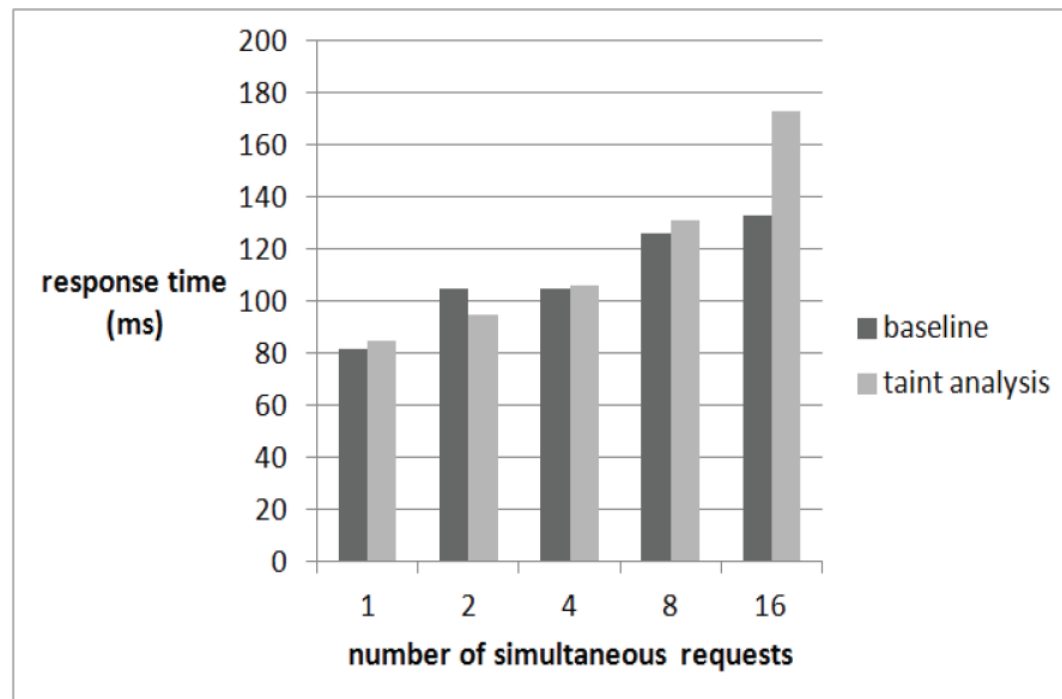
```
public aspect Guard {
    pointcut methodCalls():
        execution(* Authentication.*(..));

    Object around(): methodCalls() {
        ClassPool clPool=ClassPool.getDefault();

        byte[] initHash =
            (byte[]) codeHash.get("Authentication");
        byte[] hash;
        try {
            CtClass cls =
                clPool.get("Authentication");
            byte[] bytecode = cls.toBytecode();
            MessageDigest messageDigest =
                MessageDigest.getInstance("SHA-256");
            messageDigest.update(bytecode);
            hash = messageDigest.digest();
            return proceed();
        }
        finally {
            if (java.util.Arrays.equals
                (hash, initHash)) {
                System.out.println("true_hash_value");
            }
            else {
                reportTamper();
            }
        }
    }
}
```

AOP monitoring performance

- Experiments with “taint analysis” module implemented using AOP, which monitors behavior of a service.
- Especially useful for ITS components such as road-side units (RSUs) contacted by many vehicles during operation.
- Negligible monitoring overhead observed



Related Work

A. Attribute-based Encryption

- Ciphertext-Policy ABE (CP-ABE)
 - access policy is included in the ciphertext [10]
 - requires an access tree based on the attributes of data
 - Computationally expensive [12]

B. Vehicle Image Classification: Sighthound [8]

- Vehicle make, model, and color recognition system
- Relies on a deep convolutional neural network
- We utilize Sighthound JavaScript API [14] to retrieve results from the classifier

Related Work

C. Secure Data Exchange in V2X networks

- European (ETSI) and American (WAVE) standards for vehicles data privacy
 - anonymity, pseudonymity, unlinkability, unobservability of vehicles data (ETSI) [15]
- EPICS [16]
 - Protects data privacy by using Active Bundle [1], [2], [3]
 - Incorporates encrypted datasets, access control policies, specified by data owner, and policy execution monitor

Related Work

D. On-the-fly local data analysis

- Decentralized data neural network [17]
 - only transfers gradients (not the data) calculated through backpropagation
 - provides privacy-preserving data analytics
- Decentralized data analysis with MEMS hardware
 - data acquisition and processing are performed at local MEMS sensor nodes [18]
 - results alone are transmitted and used for decision processes at the central node

References

- [1] L. B. Othmane, “Active bundles for protecting confidentiality of sensitive data throughout their lifecycle”, Ph.D dissertation. Western Michigan University, 2010.
- [2] R. Ranchal, “Cross-domain data dissemination and policy enforcement”, Ph.D dissertation. Purdue University, 2015.
- [3] L. Lilien and B. Bhargava, “A scheme for privacy-preserving data dissemination,” IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans, vol. 36, no. 3, pp. 503–506, 2006.
- [4] D. Ulybyshev, B. Bhargava, M. Villarreal-Vasquez, A. O. Alsalem, D. Steiner, L. Li, J. Kobes, H. Halpin, and R. Ranchal, “Privacy-preserving data dissemination in untrusted cloud,” in Cloud Computing (CLOUD), 2017 IEEE 10th International Conference on IEEE, 2017, pp. 770–773.
- [5] C. Qu, D. A. Ulybyshev, B. K. Bhargava, R. Ranchal, and L. T. Lilien, “Secure dissemination of video data in vehicle-to-vehicle systems,” in Reliable Distributed Systems Workshop (SRDSW), 2015 IEEE 34th Symposium on. IEEE, 2015, pp. 47–51.
- [6] D. Ulybyshev, A. Alsalem, and B. Bhargava, “Secure data exchange and data leakage detection in untrusted cloud,” in ICACCT, 2018. Accepted, in-press.
- [7] Dr. Dobb’s Journal of Software Tools (2000). OpenCV. Key: citeulike:2236121
- [8] A. Dehghan, S. Z. Masood, G. Shu, and E. G. Ortiz, “View Independent Vehicle Make, Model and Color Recognition Using Convolutional Neural Network,” pp. 1–7, 2017.
- [9] V. Goyal, O. Pandey, A. Sahai, and B. Waters, “Attribute-based Encryption for Fine-grained Access Control of Encrypted Data,” Proceedings of the 13th ACM Conference on Computer and Communications Security, pp. 89–98, 2006.
- [10] J. Bethencourt, A. Sahai, and B. Waters, “Ciphertext-policy attribute-based encryption,” Proceedings - IEEE Symposium on Security and Privacy, pp. 321–334, 2007.

References

- [11] D. Ulybyshev, A. Alsalem, B. Bhargava, S. Savvides, G. Mani, and L. Ben-Othmane, "Secure data communication in autonomous v2x systems," in IEEE ICIOT, 2018. Accepted, in-press.
- [12] V. Kumar and S. Madria, "Distributed Attribute Based Access Control of Aggregated Data in Sensor Clouds," 2015 IEEE 34th Symposium on Reliable Distributed Systems (SRDS), pp. 218–227, 2015.
- [13] D. Liu and Y. Wang, "Monza: Image Classification of Vehicle Make and Model Using Convolutional Neural Networks and Transfer Learning," 2016.
- [14] "Sighthound." [Online]. Available: <https://www.sighthound.com/products/cloud>
- [15] "Standard: ETSI - TS 102 941. Intelligent Transport Systems (ITS); Security; Trust and Privacy Management." [Online]. Available: <https://standards.globalspec.com/std/1530232/etsi-ts-102-941>
- [16] R. Ranchal, B. Bhargava, P. Angin, and L. B. Othmane, "EPICS: A framework for enforcing security policies in composite web services," IEEE Transactions on Services Computing, 2018.
- [17] N. Lewis, S. Plis, and V. Calhoun, "Cooperative learning: Decentralized data neural network," in Neural Networks (IJCNN), 2017 International Joint Conference on. IEEE, 2017, pp. 324–331.
- [18] E. Uhlmann, A. Laghmouchi, C. Geisert, and E. Hohwieler, "Decentralized data analytics for maintenance in industrie 4.0," Procedia Manufacturing, vol. 11, pp. 1120–1126, 2017.
- [19] "Secure Data Dissemination prototype demo video." [Online]. Available: <https://www.dropbox.com/s/4wg3vuv52j4s16v/NGCRC-2017-Bhargava-Demo1.wmv?dl=0>
- [20] M. Villarreal-Vazquez, B. Bhargava, P. Angin, "Adaptable Safety and Security in V2X Systems", IEEE ICIOT 2017, paper presentation slides
- [21] "Car Dataset." [Online]. Available: https://ai.stanford.edu/jkrause/cars/car_dataset.html
- [22] M. Castrillón-Santana, O. Déniz-Suárez, L. Antón-Canalís, and J. Lorenzo-Navarro. "Face and facial feature detection evaluation performance evaluation of public domain haar detectors for face and facial feature detection." (2008)