Lightweight Secure Communication Protocol for IoV

Dr. Debasis Das
Department of Computer Science and Engineering
IIT Jodhpur

Intelligent Transport System (ITS)

- Advanced vehicles and associated transportation infrastructures that use IT&C technology to make driving safer, efficient and comfortable

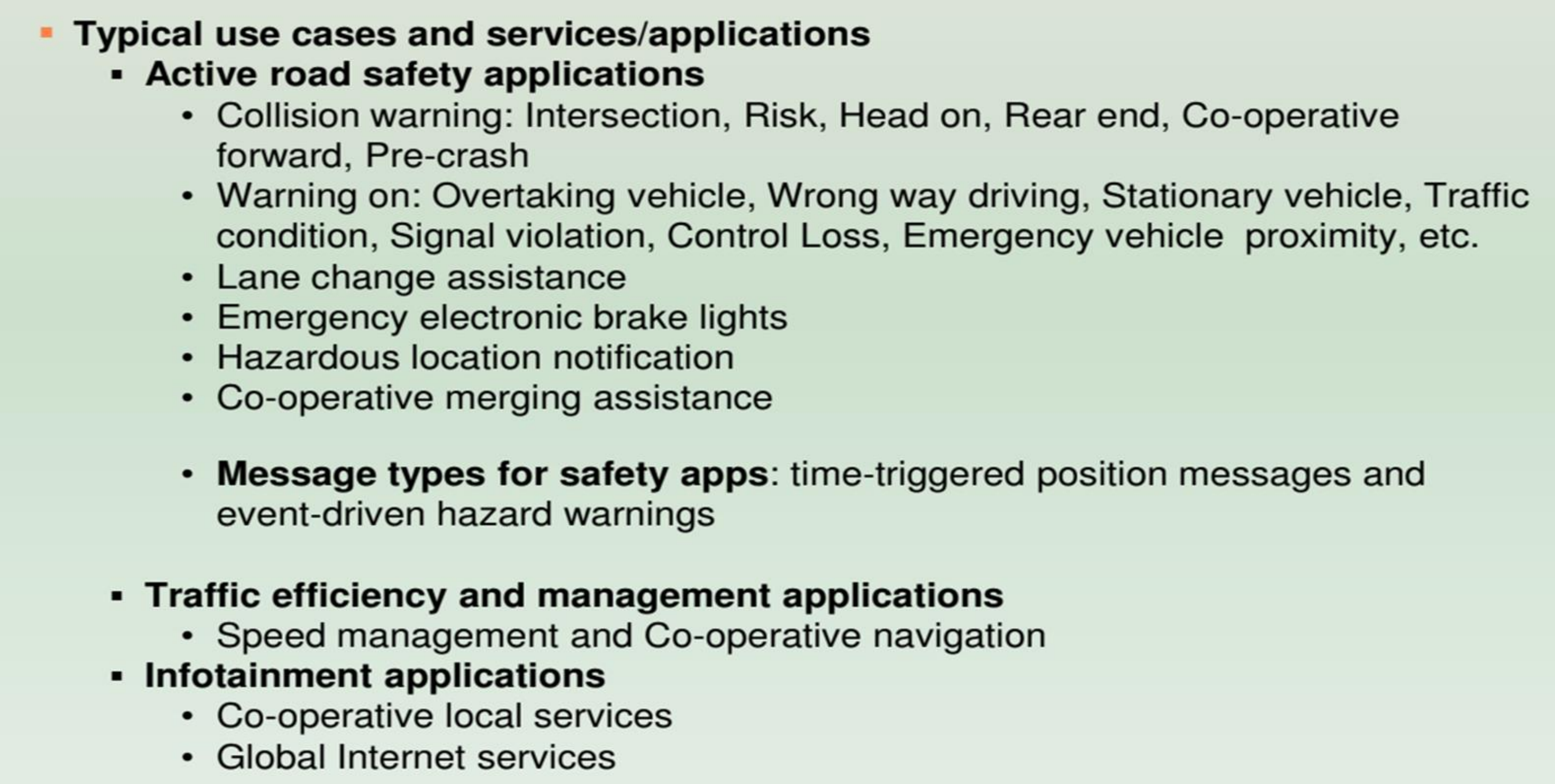
- Operation of vehicles, manage vehicle traffic, assist drivers with safety and other information, provisioning of convenience applications for passengers

- ITS
  - high interest for companies, operators, government, academia, research; many countries have public and private sector bodies working on ITS

  - Important technologies - implementing many applications related to vehicles, vehicle traffic, drivers, passengers and pedestrians

- **Typical use cases and services/applications**
  - **Active road safety** applications
    - Warnings, notifications, assistance
  - **Traffic efficiency** and management applications
  - **Infotainment** applications

Intelligent Transport System (ITS)



- **Typical use cases and services/applications**
  - **Active road safety applications**
    - Collision warning: Intersection, Risk, Head on, Rear end, Co-operative forward, Pre-crash
    - Warning on: Overtaking vehicle, Wrong way driving, Stationary vehicle, Traffic condition, Signal violation, Control Loss, Emergency vehicle proximity, etc.
    - Lane change assistance
    - Emergency electronic brake lights
    - Hazardous location notification
    - Co-operative merging assistance

    - **Message types for safety apps**: time-triggered position messages and event-driven hazard warnings

  - **Traffic efficiency and management applications**
    - Speed management and Co-operative navigation
  - **Infotainment applications**
    - Co-operative local services
    - Global Internet services

Vehicular Ad-Hoc Networks(VANETs)

- Recent advances in **hardware, software, and communication** technologies are enabling the **design and implementation** of a whole range of different types of networks that are being deployed in various environments.

- One such network that has received a lot of interest in the last couple of years is the **Vehicular Ad-Hoc Network (VANET).**

- VANET has become an active area of **research, standardization, and development because it has tremendous potential** to **improve vehicle and road safety, traffic efficiency, and convenience as well as comfort to both drivers and passengers.**

Introduction

- Vehicular communications are used in various **safety and business applications in today's technology world for user benefits.**

- In this, **vehicle-to-vehicle (V2V) and V2R** communication enables **users to exchange meaningful information with nearby vehicles directly**.

- In general, **vehicles move faster on the highway rather than the intersection road environment**, and thus, **a robust system is required to communicate efficiently and securely.**

Motivation

- The traditional **Intelligent Transport System (ITS)** has significantly evolved, including **vehicular communication and networks**
  - Main communications: V2V, V2R, V2I→ Vehicular ad-hoc Networks (VANET)

- VANET (special class of Mobile ad-hoc Network - MANET)
  - has both **technical and business-related limitations**
  - still - **not very large scale deployment in the world**

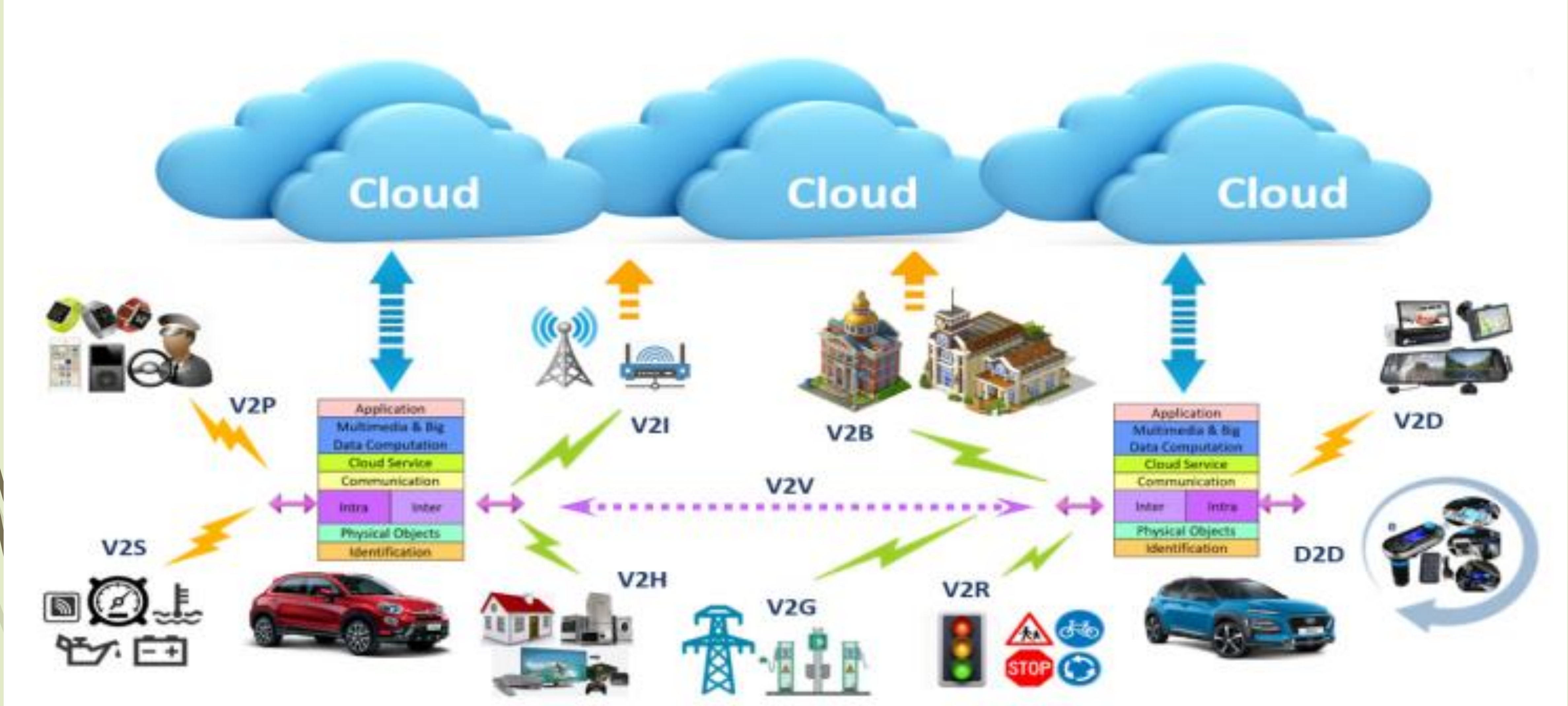
Dedicated Short Range Communications (DSRC) protocol

- According to the Dedicated Short Range Communications (DSRC) protocol, each vehicle in a **VANET broadcasts a traffic safety message every 100-300ms,**
- Which keeps the vehicle’s **driving related information, such as location, speed, turning intention, and driving status** (e.g., **regular driving, waiting for a traffic light, traffic jam, etc.),** to other vehicles.

Objective

- To present a **new universal architecture for the Vehicular Networks** which can be used for **different and communication models, large-scale data sensing, collection, information processing**, storage **with an emphasis on deployment in smart cities to address the following challenges like driver safety, traffic efficiency, and infotainment, etc.**

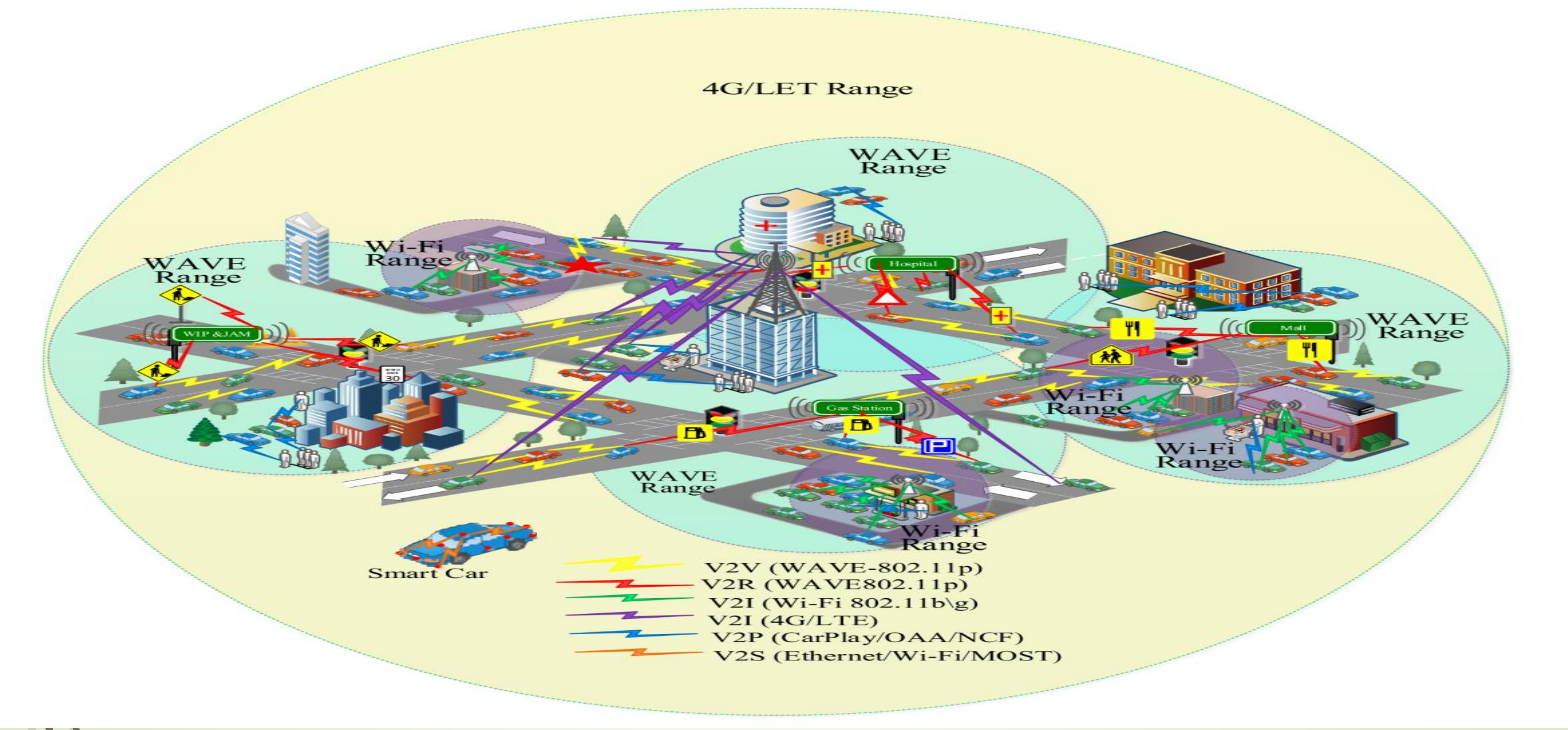
Universal VANETs



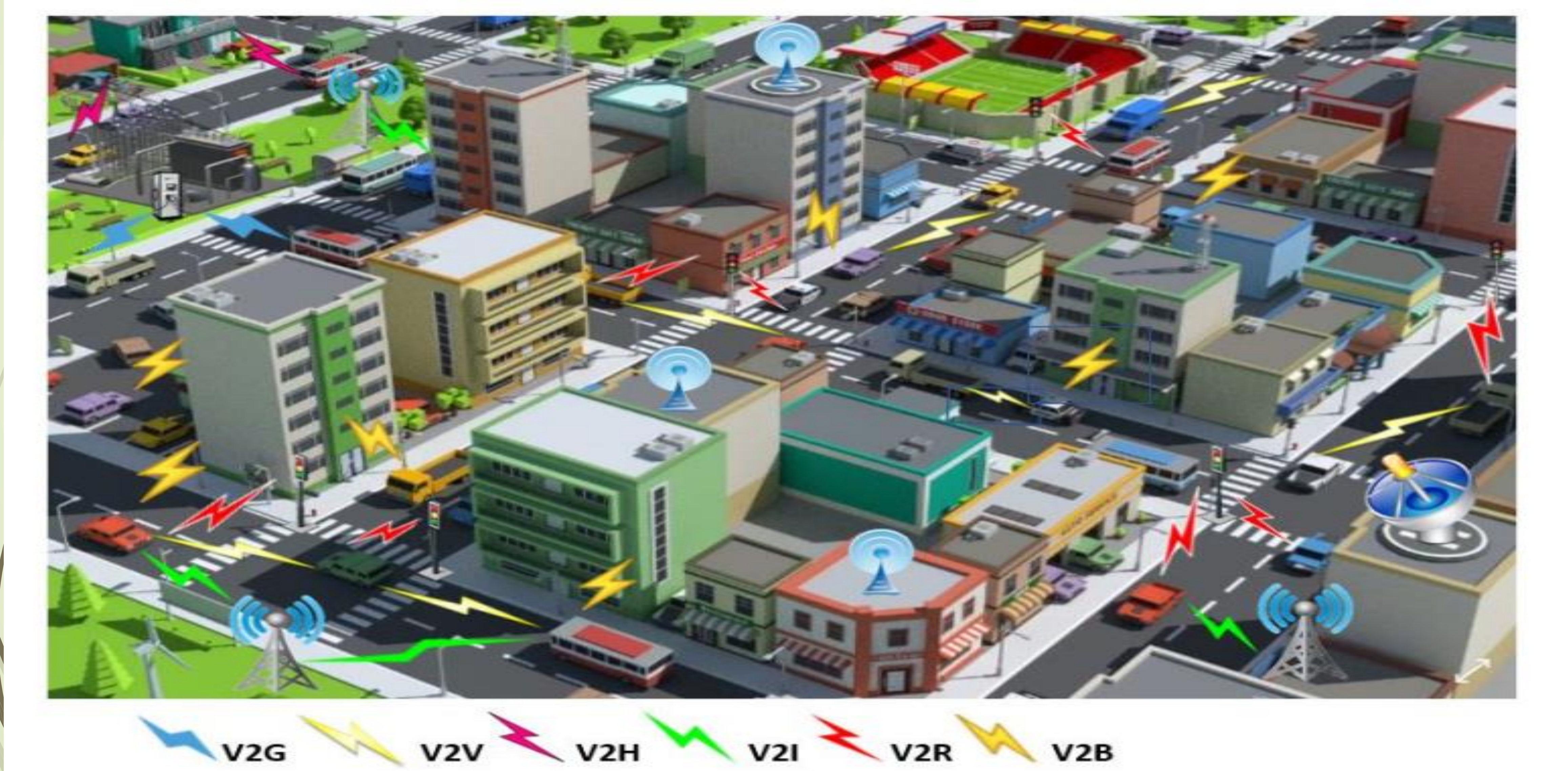
Application
Multimedia & Big Data Computation
Cloud Service
Communication
Intra | Inter
Physical Objects
Identification

Application
Multimedia & Big Data Computation
Cloud Service
Communication
Inter | Intra
Physical Objects
Identification

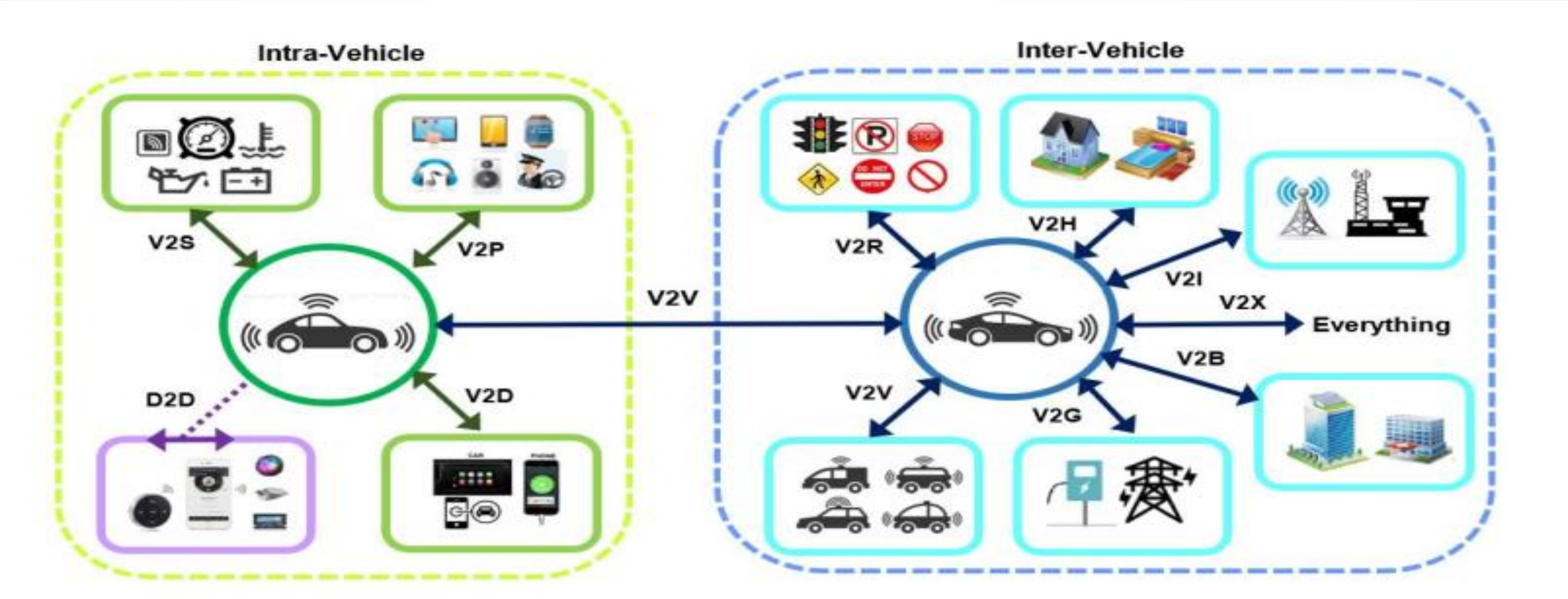
The realization of Universal VANETs with heterogeneous vehicular networks



Universal VANETs interactions for smart cities



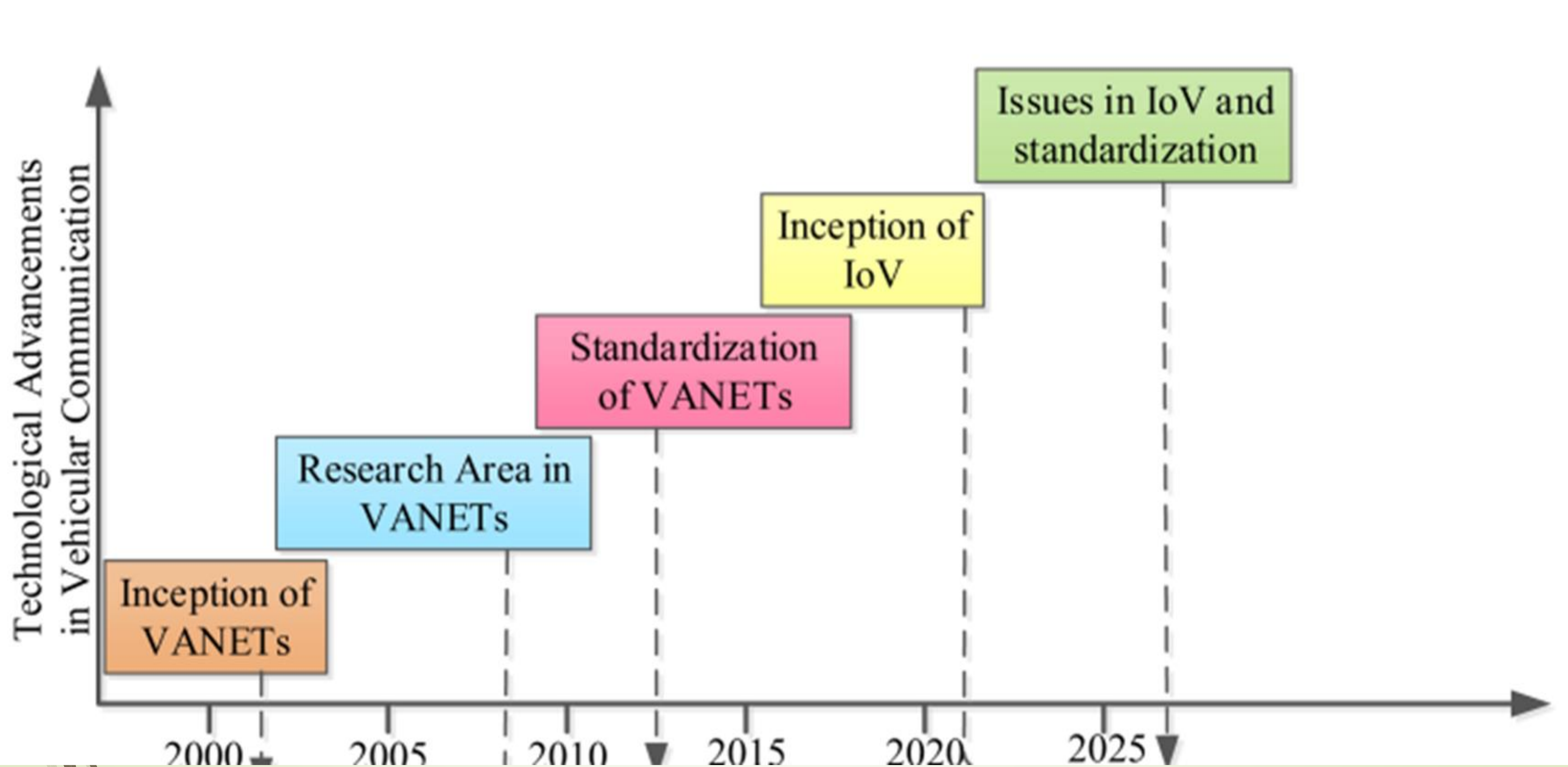
Interaction Models of Universal VANETs



Why Universal VANETs(or IoV)

- The number of on-road vehicles has been **predicted to increase significantly in the world.**
- **Due to the higher motorization rate, congestion would result in longer** on-road travelling time in coming years.
- Studies **show that about 60%** of roadway accidents could be avoided if the driver of the vehicle was **provided warning at least one-half second prior to a collision**
- Even if 5 minutes of the time wasted in travelling globally is monetized then **it is expected to generate Euro 25 billion revenue per year by 2030**.
- Automobile industry is expected to increase the profit margin of Euro **54 billion in 2012 to Euro 79 billion by 2020.**

Evolution of vehicular communication from VANETs towards IoV

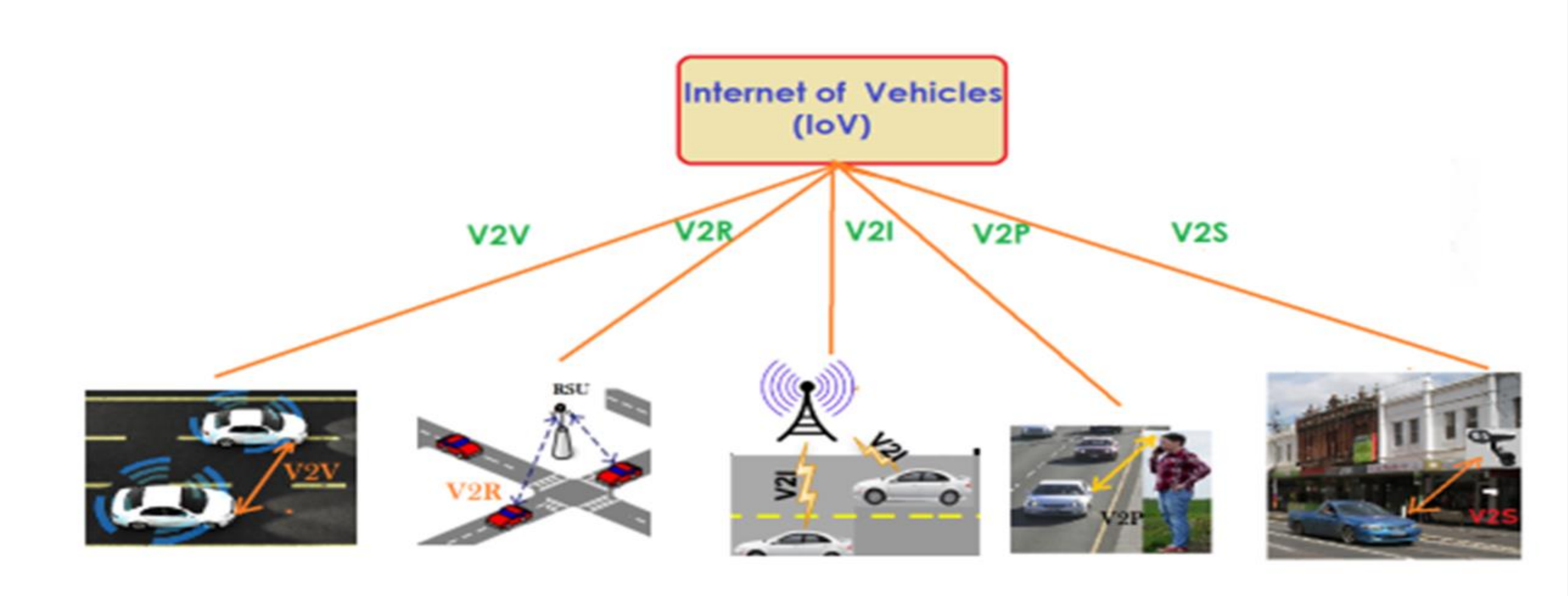


Technological Advancements in Vehicular Communication
Inception of VANETs
Research Area in VANETs
Standardization of VANETs
Inception of IoV
Issues in IoV and standardization
2000
2005
2010
2015
2020
2025

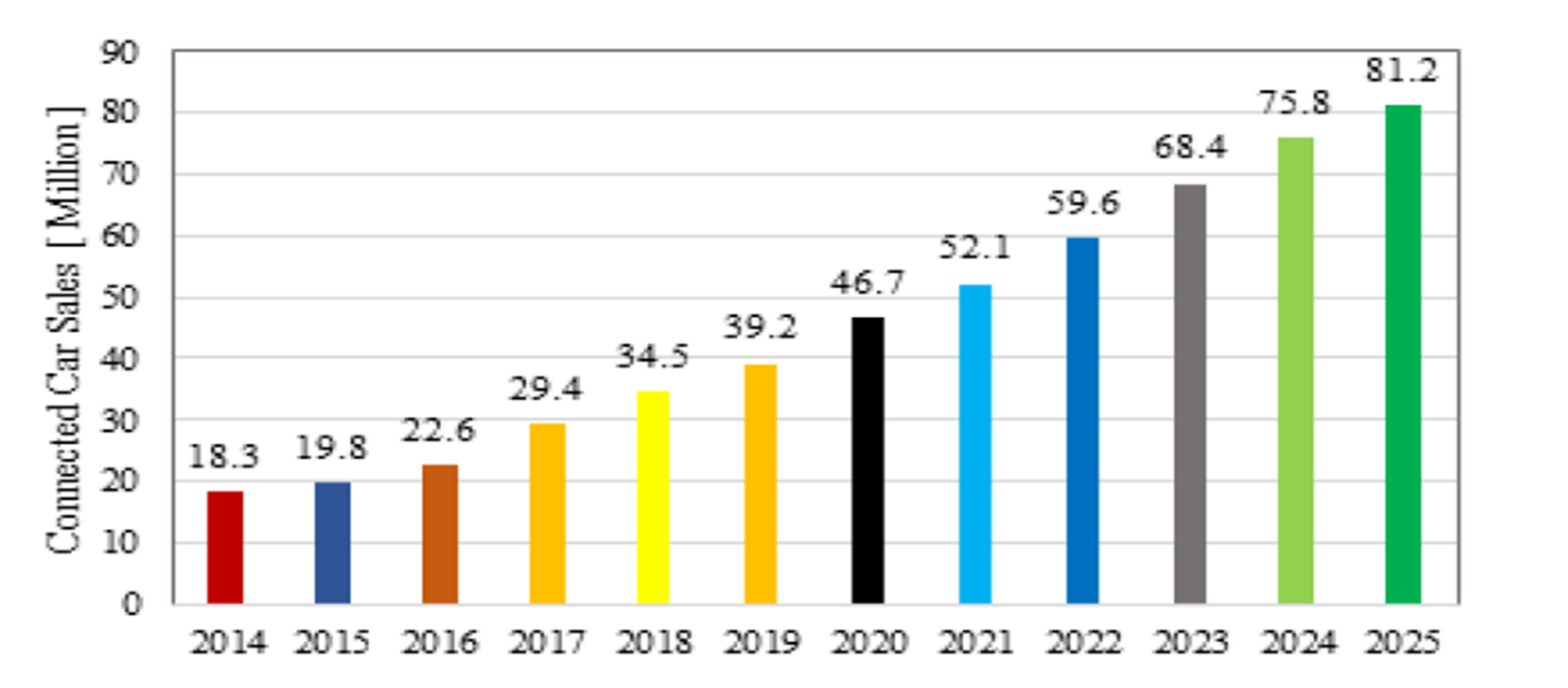
Internet of Vehicles(IoV)

- The Internet of Vehicles (IoV) is a typical application of it in the field of transportation, which aims at achieving an integrated
- **intelligent transportation system to enhance traffics**,
- **to avoid accidents,**
- **to ensure road safety, and**
- **to improve driving experiences.**

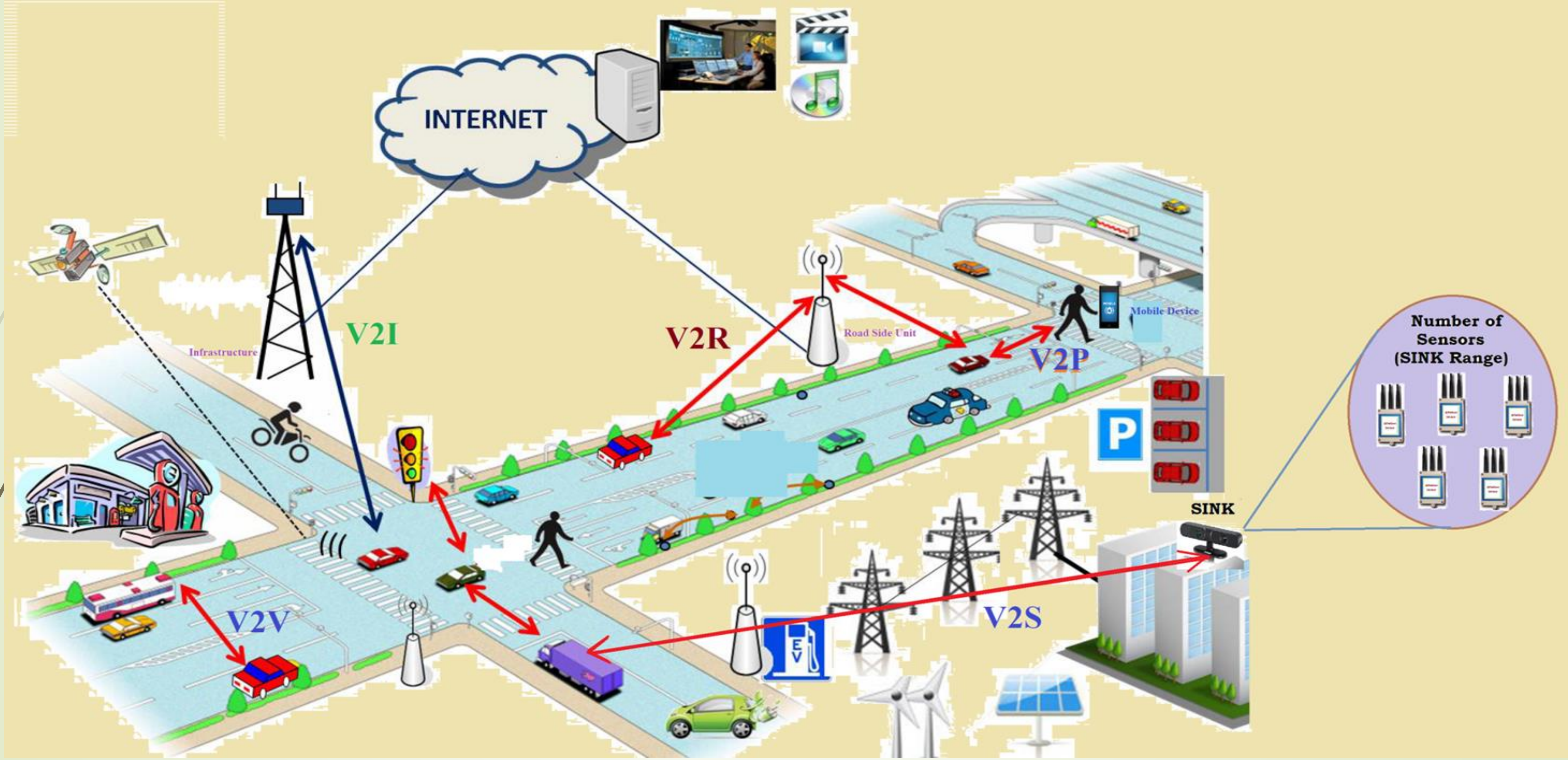
Internet of Vehicles(IoV) [VANETs + IoT]



The prediction of car sales with some form of connectivity till 2025 [16].



Internet of Vehicles(IoV) communication environment



Benefits of Universal VANETs

- The vehicular communications of IoV would be **highly commercialized**.

- This is due to the **smart commercial and infotainment applications** in addition to the **smart safety, management and efficiency applications.**

- The network architecture of IoV would integrate vehicular communication with other communication networks. This is due to the **heterogeneous network architecture.**

- IoV would provide reliable Internet service in vehicles. This is due to the inclusion of **V2I communication**.

- Most of the **existing computing and communication devices in our daily would be compatible with vehicular networks.**

- **The processing and decision making capability of vehicles**, size of vehicular networks, volume of network data would enlarge drastically in IoV.

Projects and Standards

- Many **projects and standards** - developed all over the world: USA, Europe, Asia, etc.
- Standardization made by US Federal Communications Communication (FCC)
  - allocation of 75MHz of ***Dedicated Short Range Communication (DSRC)*** spectrum
  - basically for V2V and V2I communications for safety apps.

- Numerous research works and standardization/projects have been performed
- **Examples:**
  - **DSRC** development by Vehicle Safety Communications Consortium (VSCC) (USA)
  - European automotive industry project dedicated to road safety development and demo - **PReVENT** project (Europe) 2004-2008
  - Internet intelligent transportation system (ITS) **Consortium and Advanced Safety Vehicle** project (Japan), 2011-2015
  - **Car-2-Car** Communications Consortium (C2C-CC), ETSI TC ITS
  - **Vehicle Infrastructure Integration** (VII) Program- USA 2009
  - Secure Vehicle Communication (**SeVeCOM**) - FP6 Europe, 2006-2008
  - **Network on Wheels** project (Germany), 2008, etc.

Market Opportunities

- The VANETs offers huge market opportunity not only for automobile industry **(like, Visteon Corporation, Ford, Audi, BMW etc) ,** but also for a range of other industries including IT equipment manufacturer **(like Dell, Intel, Qualcomm, Unex Technology Corporation etc)** software **industry (Like Microsoft, Google, CTS, TCS, Wipro, Microsoft, Honeywell etc)** and Internet service providers**(like Vodafone).**

Research Opportunities

- Recently, researchers have **designed various message dissemination schemes**, but different concerns **(i.e., security threats, more execution time, high communication overhead, and storage cost)** are present in these systems, and this leads **to unreliability for on-road communication**.

Security

- In information technology, *security* is the protection of information assets through the use of technology, processes, and training.

What is network security?

confidentiality: only sender, intended receiver should "understand" message contents

- sender encrypts message
- receiver decrypts message

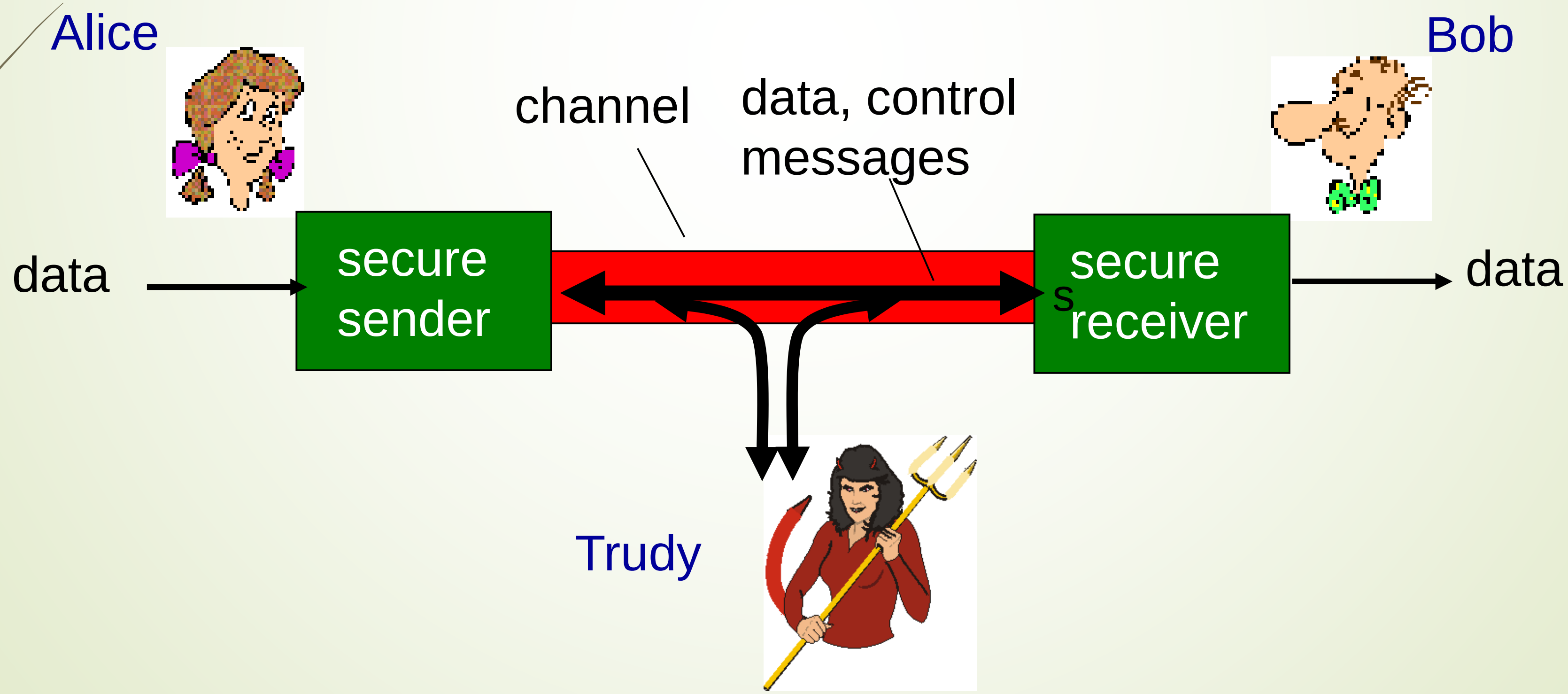
authentication: sender, receiver want to confirm identity of each other

message integrity: sender, receiver want to ensure message not altered (in transit, or afterwards) without detection

access and availability: services must be accessible and available to users

Friends and enemies: Alice, Bob, Trudy

- well-known in network security world Bob, Alice (Friend) want to communicate “securely”
- Trudy (intruder) may intercept, delete, add messages



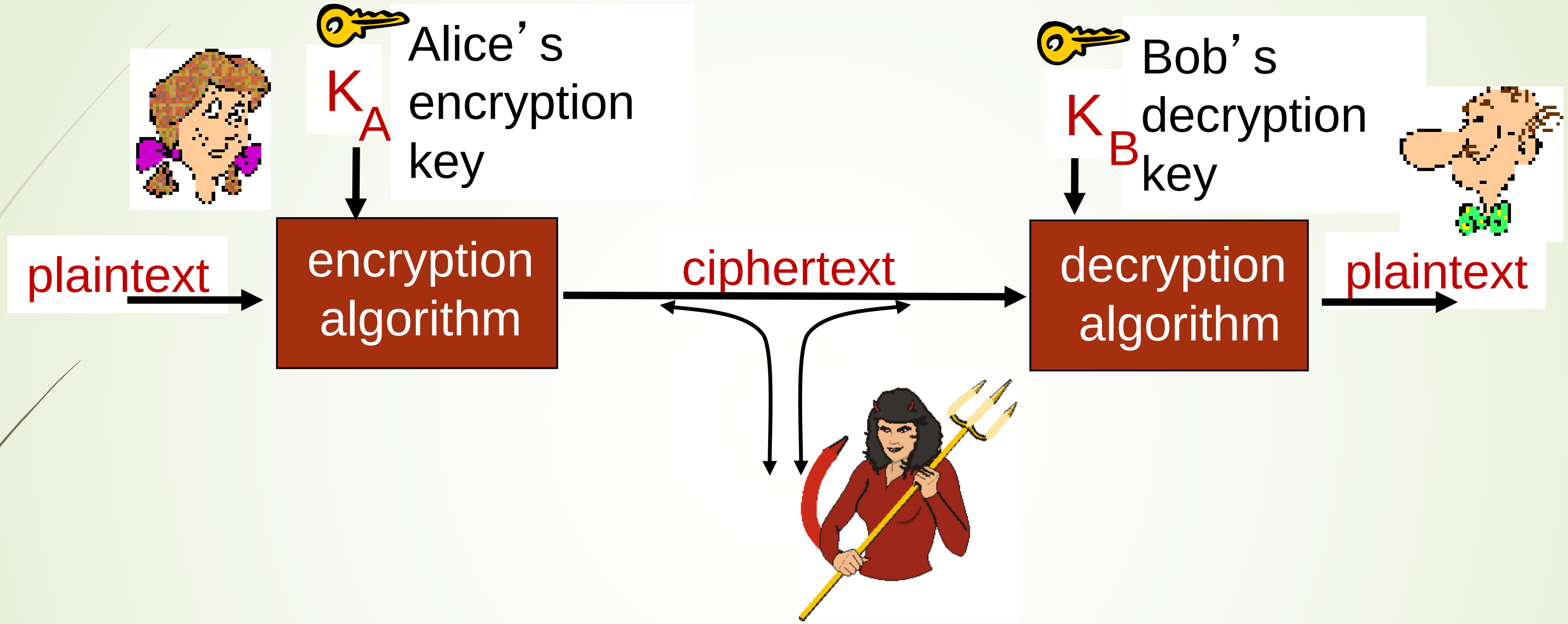
Who might Bob, Alice be?

- well, *real-life* Bobs and Alices!
- Web browser/server for electronic transactions (e.g., on-line purchases)
- on-line banking client/server
- DNS servers
- routers exchanging routing table updates
- other examples?

There are bad guys out there!

- What can a “bad guy” do?
- *A:* A lot! See section 1.6
  - *eavesdrop:* intercept messages
  - actively *insert* messages into connection
  - *impersonation:* can fake (spoof) source address in packet (or any field in packet)
  - *hijacking:* “take over” ongoing connection by removing sender or receiver, inserting himself in place
  - *denial of service:* prevent service from being used by others (e.g., by overloading resources)

Principles of cryptography

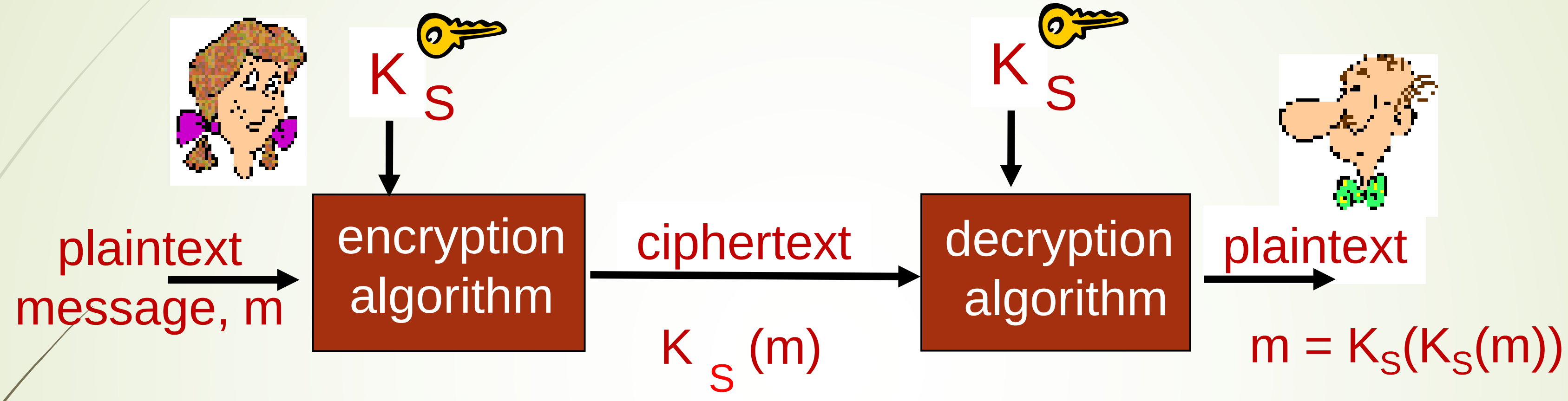


m plaintext message

$K_A(m)$ ciphertext, encrypted with key K_A

$m = K_B(K_A(m))$

Symmetric key cryptography



symmetric key crypto: Bob and Alice share same (symmetric) key: K

S

- e.g., key is knowing substitution pattern in mono alphabetic substitution cipher

Q: how do Bob and Alice agree on key value?

Simple encryption scheme

substitution cipher: substituting one thing for another

- monoalphabetic cipher: substitute one letter for another

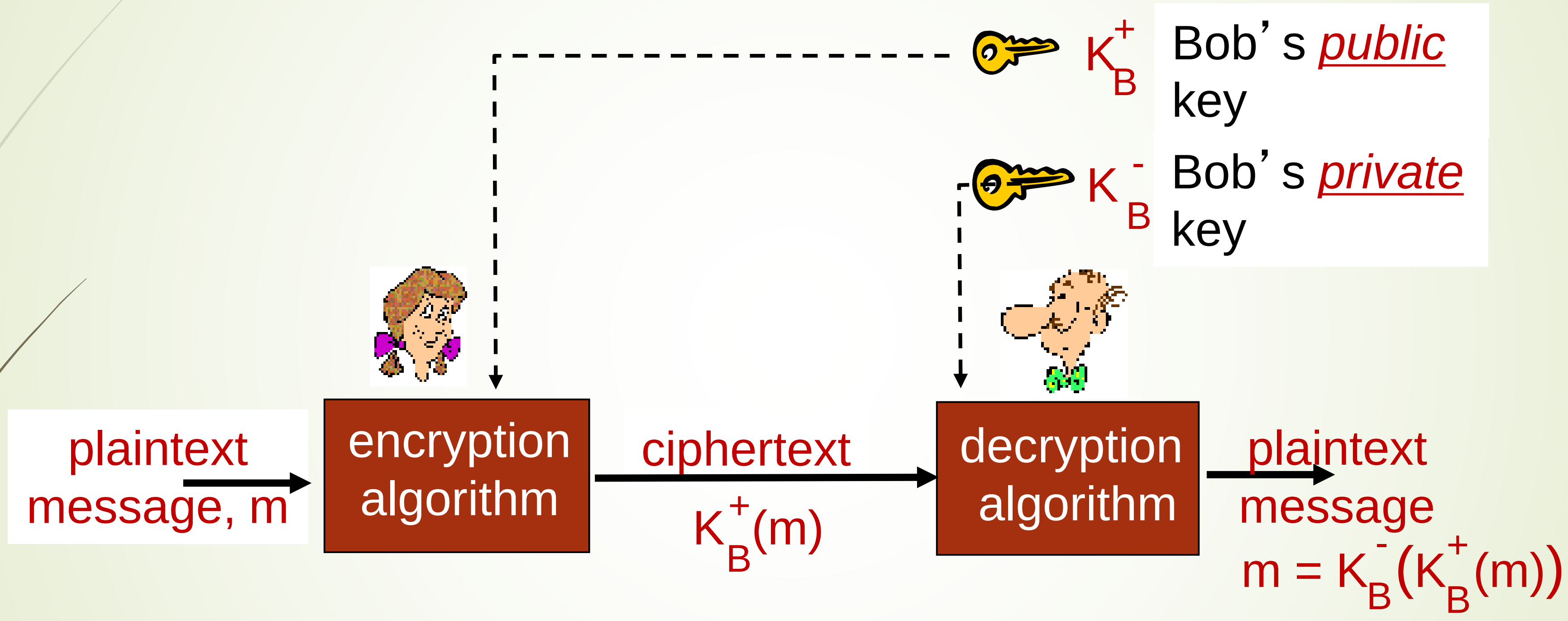
```
plaintext:   abcdefghijklmnopqrstuvwxyz

ciphertext:  mnbvcxzasdfghjklpoiuytrewq
```

e.g.:

```
 Plaintext: bob. i love you. alice
ciphertext: nkn. s gktc wky. mgsbc
```

Encryption key: mapping from set of 26 letters to set of 26 letters

Public key cryptography



K_B^+ Bob's *public* key

K_B^- Bob's *private* key

plaintext message, m

encryption algorithm

ciphertext

$K_B^+(m)$

decryption algorithm

plaintext message

$m = K_B^-(K_B^+(m))$

Public key encryption algorithms

requirements:

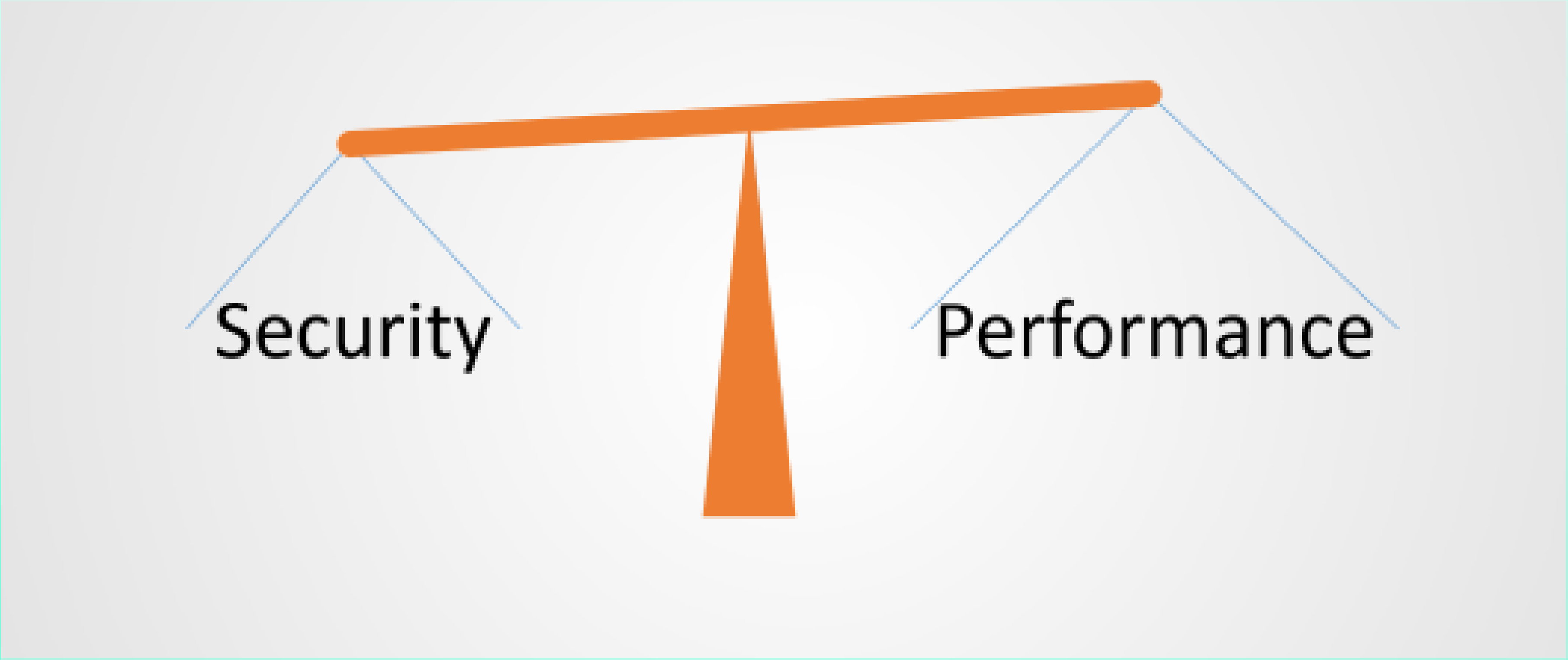
1 need $K_B^+(\cdot)$ and $K_B^-(\cdot)$ such that

$$K_B^-(K_B^+(m)) = m$$

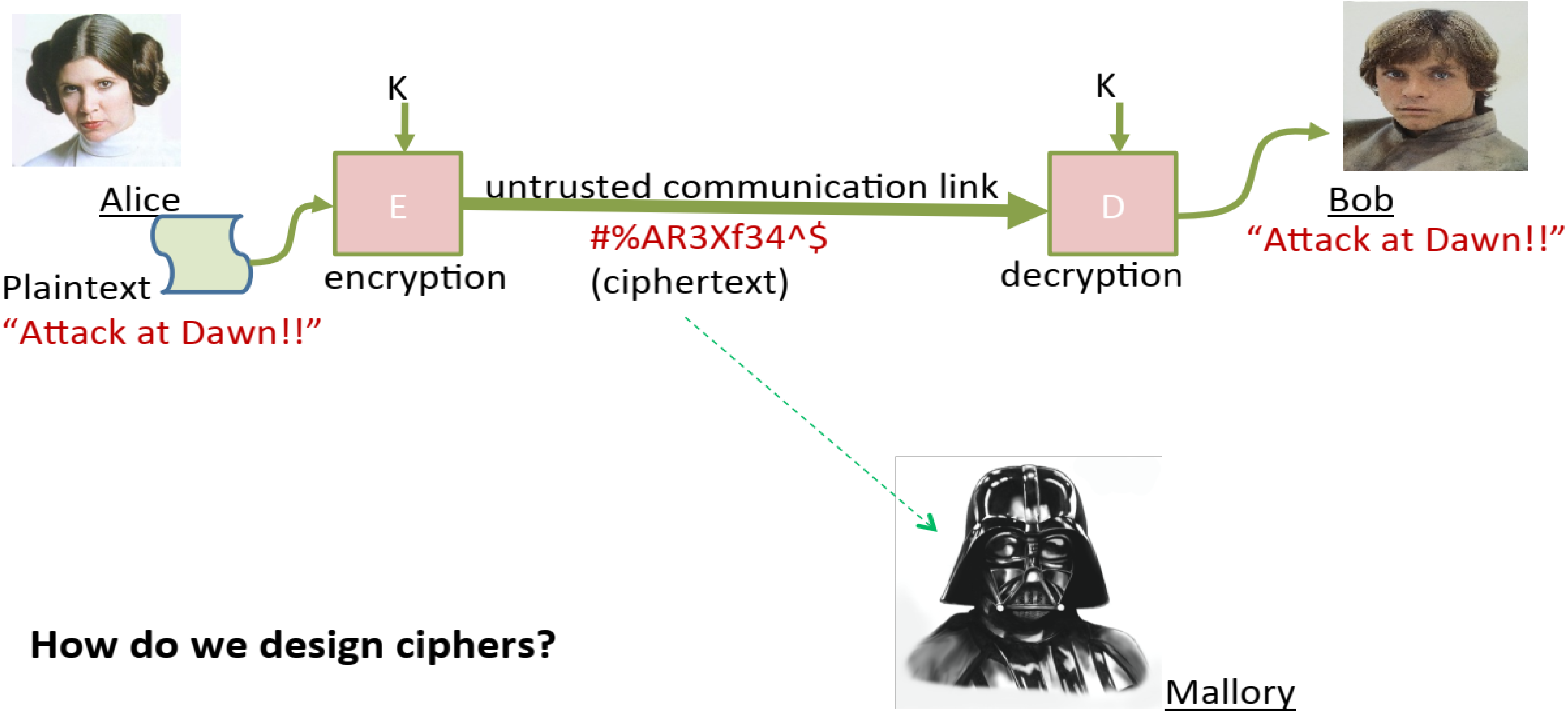
2 given public key K_B^+, it should be impossible to compute private key K_B^-

RSA: Rivest, Shamir, Adelson algorithm

Security-Performance Tradeoff



Encryption



K

K

Alice

Plaintext

“Attack at Dawn!!”

E

encryption

untrusted communication link

#%AR3Xf34^$

(ciphertext)

D

decryption

Bob

“Attack at Dawn!!”

Mallory

How do we design ciphers?

Cipher Models
(What are the goals of the design?)

Computation Security

My cipher can withstand all attacks with complexity less than 2^{2048}

The best attacker with the best computation resources would
take 3 centuries to attack my cipher

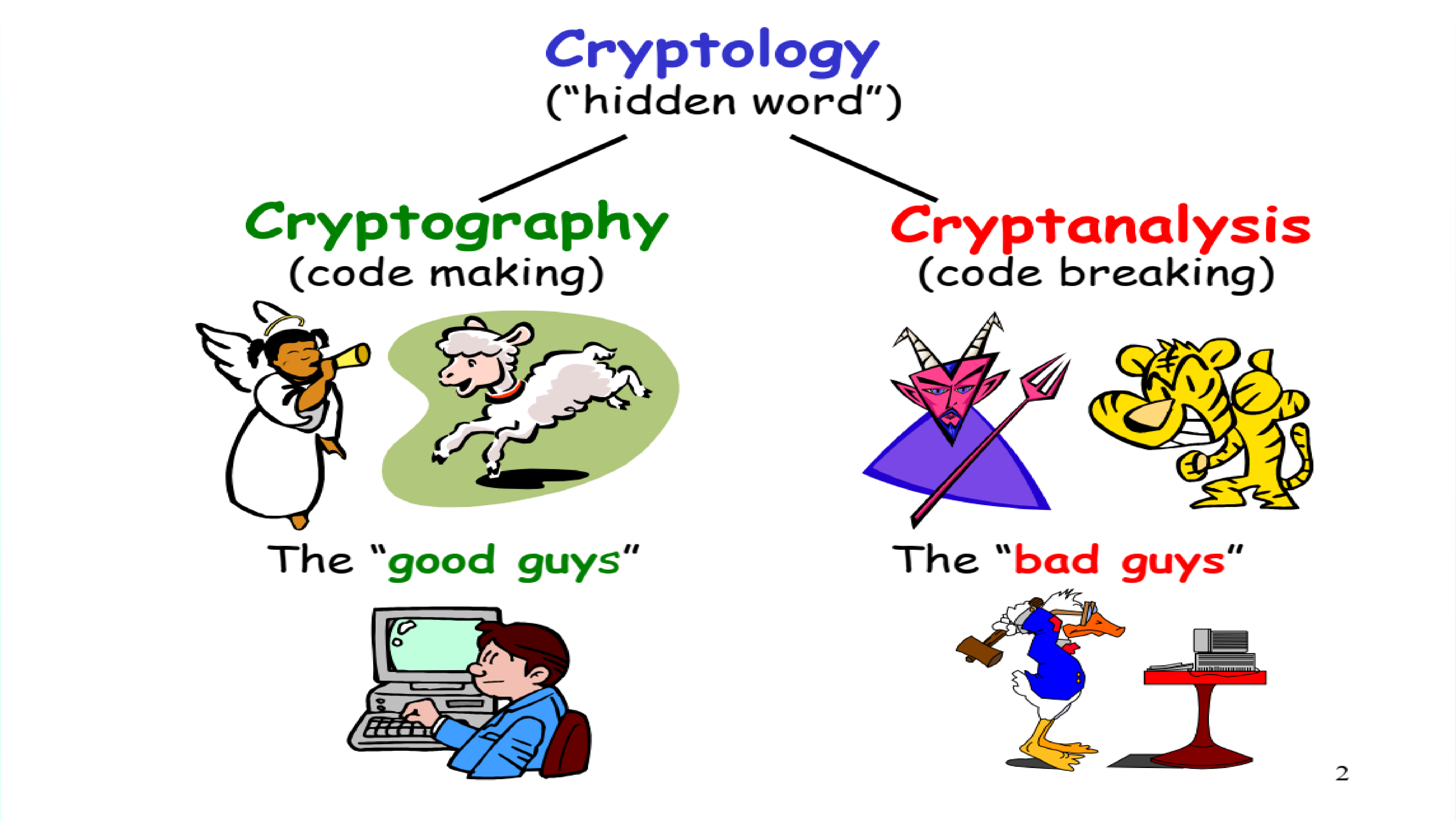
Unconditional Security

My cipher is secure against all attacks irrespective of the
attacker's power.
I can prove this!!

Provable Security (Hardness relative to a tough problem)

If my cipher can be broken then large numbers can be factored easily

This model is also known as **Perfect Secrecy.**
Can such a cryptosystem be built?
We shall investigate this.



Cryptology

("hidden word")

Cryptography

(code making)

The "good guys"

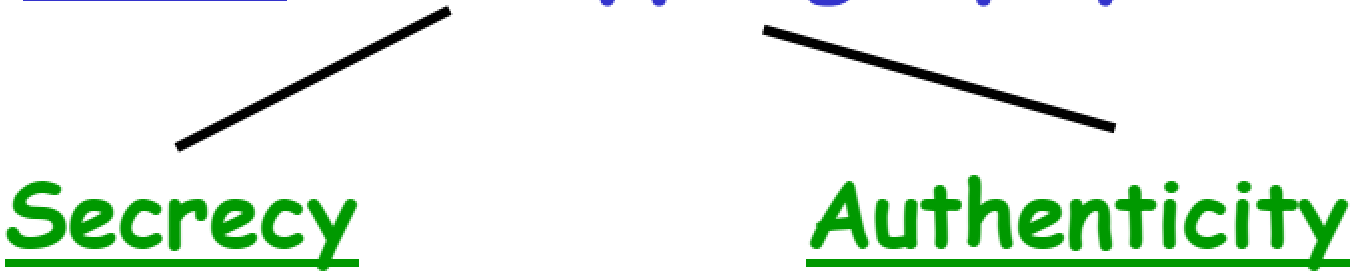
Cryptanalysis

(code breaking)

The "bad guys"

2

Goals of cryptography



Secrecy

Authenticity

Xuejia Lai has given a useful razor for deciding whether something is a matter of secrecy or a matter of authenticity.

IoVCom: Reliable Comprehensive Communication System for Internet of Vehicles

Introduction

- By 2020, around 25 billion "things" will be connected to the Internet for a better society using different technological systems.
- Vehicle users have better experience by collaborating the Internet of Things (IoT) and vehicular ad-hoc network (VANET) architectures, and this emerging field is called the **Internet of vehicles (IoV).**
- Therefore, the **IoV architecture** will play an important role in the **industry, research organization, and academics for various public and commercial applications.**
- However, the IoV structure **should ensure secure and efficient performance for vehicular communications, else an attacker may interfere in the system**

Introduction

- We propose protected **comprehensive data dissemination protocols** (say IoVCom) based on **one-way hash function and elliptic curve cryptography (ECC)** for the IoV structure.
- Next, we **analyze security** strengths of the IoVCom against various security attacks
- Discuss performance results in terms of communication **overhead, computation time, storage cost, and energy consumption.**

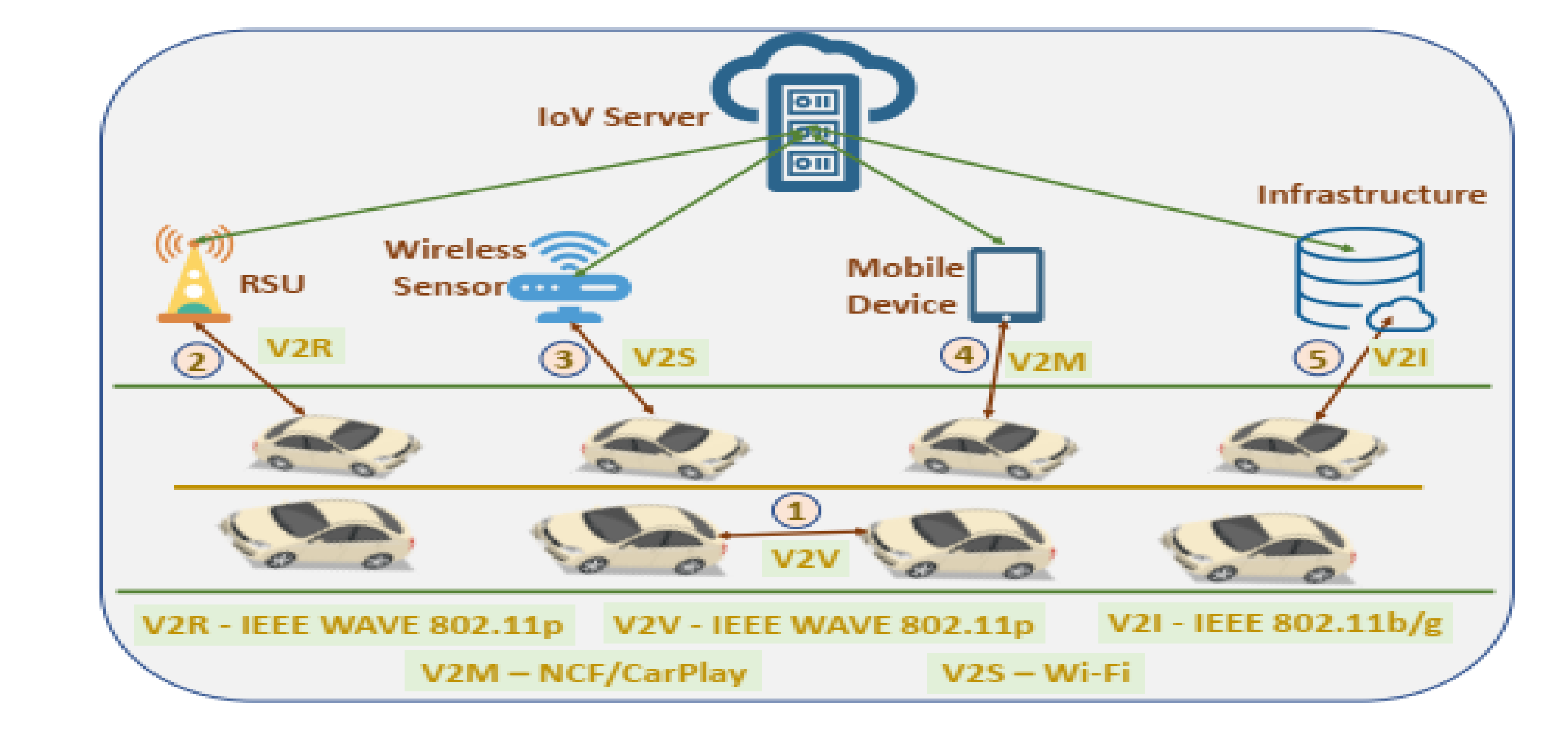
IoV Applications

- IoV applications can be broadly classified into two ways, (1) business oriented (2) safety-related.
- Business-oriented applications include car-sharing, insurance, infotainment, etc.
- Safety-related applications are navigation, remote telematics, diagnostic, traffic efficiency, co-operative message transfer, post-crash notification, enhancing traffic safety, cooperate to help other vehicles, real-time traffic, etc

Different IoV communications

- One of the key features of the IoV is its different communications (see Figure 1), **and it is systematized as V2V (vehicle-tovehicle), V2R (vehicle-to-roadside unit), V2S (vehicle-towireless sensor), V2M (vehicle-to-mobile device), and V2I (vehicle-to-infrastructure)**.
- However, these communications are carried out using different wireless access technologies (WAT).
- In general, the WAT include **Wi-Fi for V2S**, **Wi-Fi 802.11b/g** for V2I, **NCF/CarPlay** for V2M, and IEEE **WAVE 802.11p for V2V and V2R.**

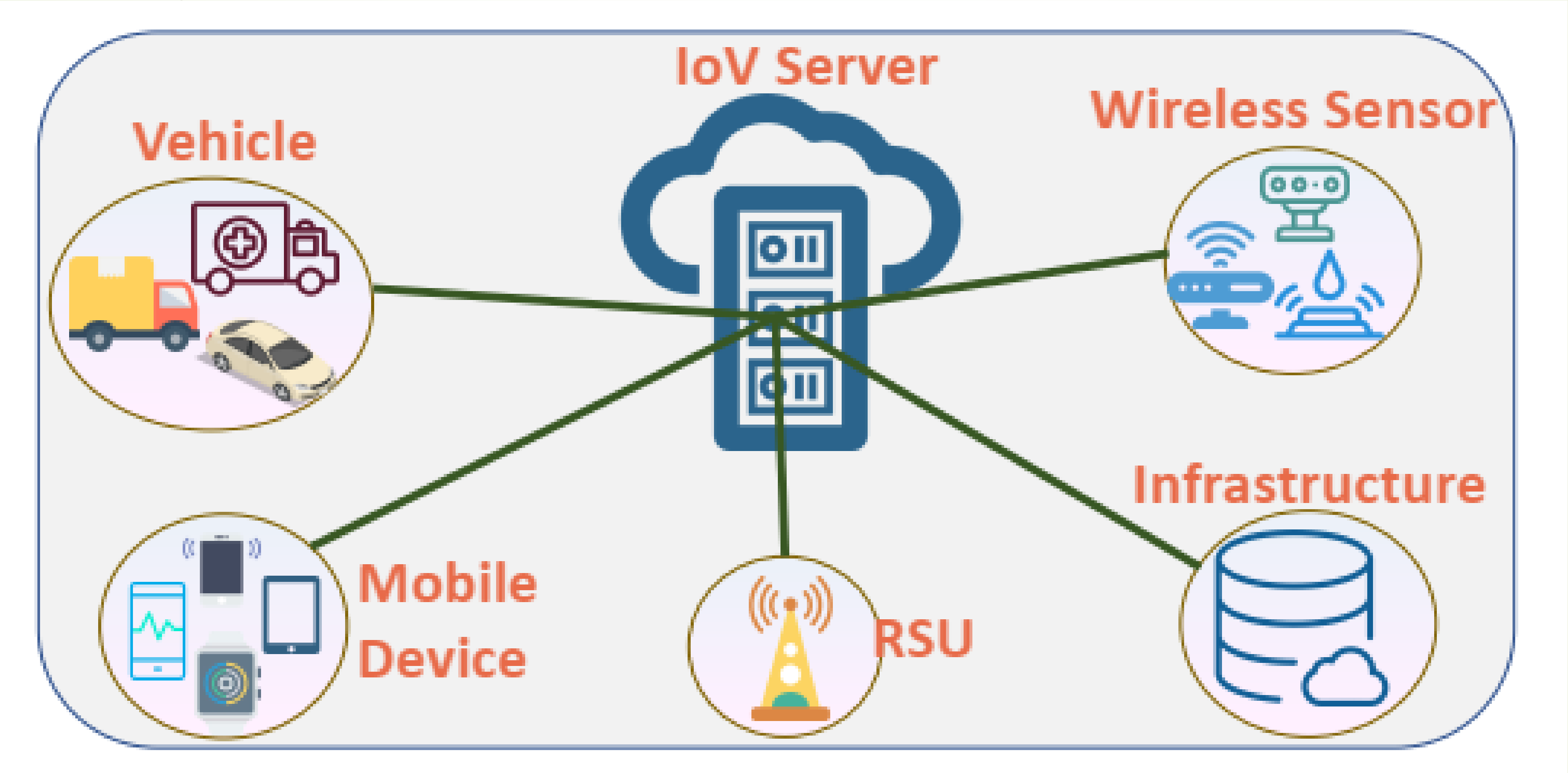
The generalized IoV communication architecture



Registration process in IoV

- **Figure 2 shows the outline of a direct link between these devices and the IoV server.**
- **In general, the registration process happens through a secure infrastructure (e.g., SSL/TLS protocol).**
- **The IoV server is the central components in the IoV architecture.**

The registration connection with the IoV server



Novel comprehensive data transmission protocols

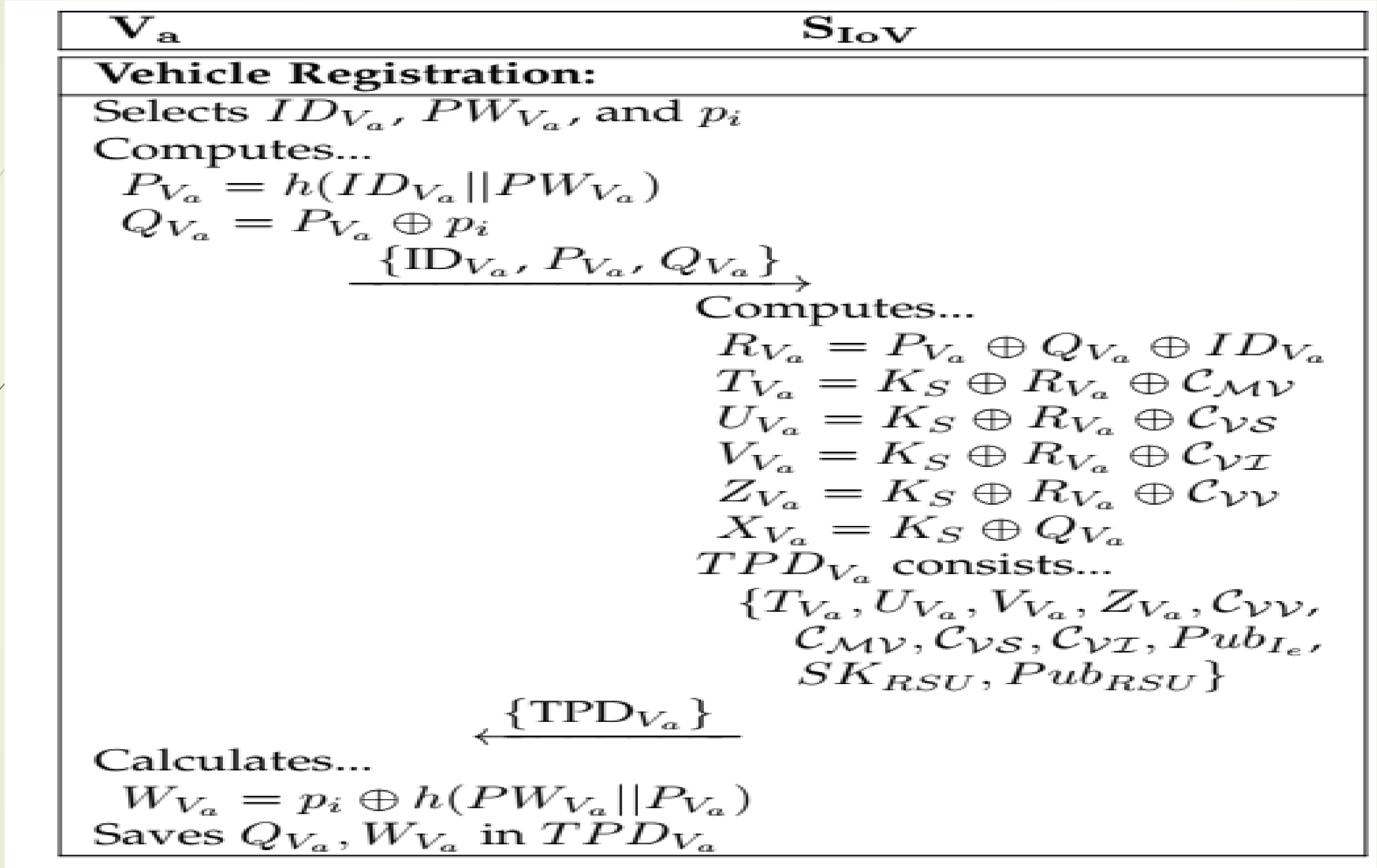
- Design a dependable system with five communications (V2S, V2V, V2I, V2M, and V2R) using one-way hash and elliptic curve operations to achieve mutual authentication between IoV entities (vehicle, RSU, mobile device, wireless sensor, and infrastructure).
- Resists various security attacks, e.g., Sybil, collision induction, modification, illusion, impersonation, replay, password guessing, man-in-the-middle, and plain-text.
- Attains better results in different performance measures such as execution time, energy consumption, storage cost, and communication overhead.

The Proposed Protocol: IovCom

- **The IoVCom: Registration and Setup**
  - ***Vehicle Registration***
  - ***Mobile user Registration***
  - ***Road-side-unit Setup***
  - ***Wireless Sensor Setup***
  - ***Infrastructure Setup***

- **The IoVCom: Data Transmission Schemes**
  - ***Vehicle-to-Vehicle***
  - ***Vehicle-to-Mobile***
  - ***Vehicle-to-RSU***
  - ***Vehicle-to-Wireless Sensor***
  - ***Vehicle-to-Infrastructure***

IoVCom: Vehicle Registration Phase



$\mathbf{V_a}$ | **$\mathbf{S_{IoV}}$**

Vehicle Registration:

Selects ID_{V_a}, PW_{V_a}, and p_i

Computes...

$P_{V_a} = h(ID_{V_a} || PW_{V_a})$

$Q_{V_a} = P_{V_a} \oplus p_i$

$$\xrightarrow{\{\mathrm{ID}_{V_a}, P_{V_a}, Q_{V_a}\}}$$

Computes...

$R_{V_a} = P_{V_a} \oplus Q_{V_a} \oplus ID_{V_a}$

$T_{V_a} = K_S \oplus R_{V_a} \oplus \mathcal{C}_{\mathcal{MV}}$

$U_{V_a} = K_S \oplus R_{V_a} \oplus \mathcal{C}_{\mathcal{VS}}$

$V_{V_a} = K_S \oplus R_{V_a} \oplus \mathcal{C}_{\mathcal{VI}}$

$Z_{V_a} = K_S \oplus R_{V_a} \oplus \mathcal{C}_{\mathcal{VV}}$

$X_{V_a} = K_S \oplus Q_{V_a}$

TPD_{V_a} consists...

$\{T_{V_a}, U_{V_a}, V_{V_a}, Z_{V_a}, \mathcal{C}_{\mathcal{VV}},$
$\mathcal{C}_{\mathcal{MV}}, \mathcal{C}_{\mathcal{VS}}, \mathcal{C}_{\mathcal{VI}}, Pub_{I_e},$
$SK_{RSU}, Pub_{RSU}\}$

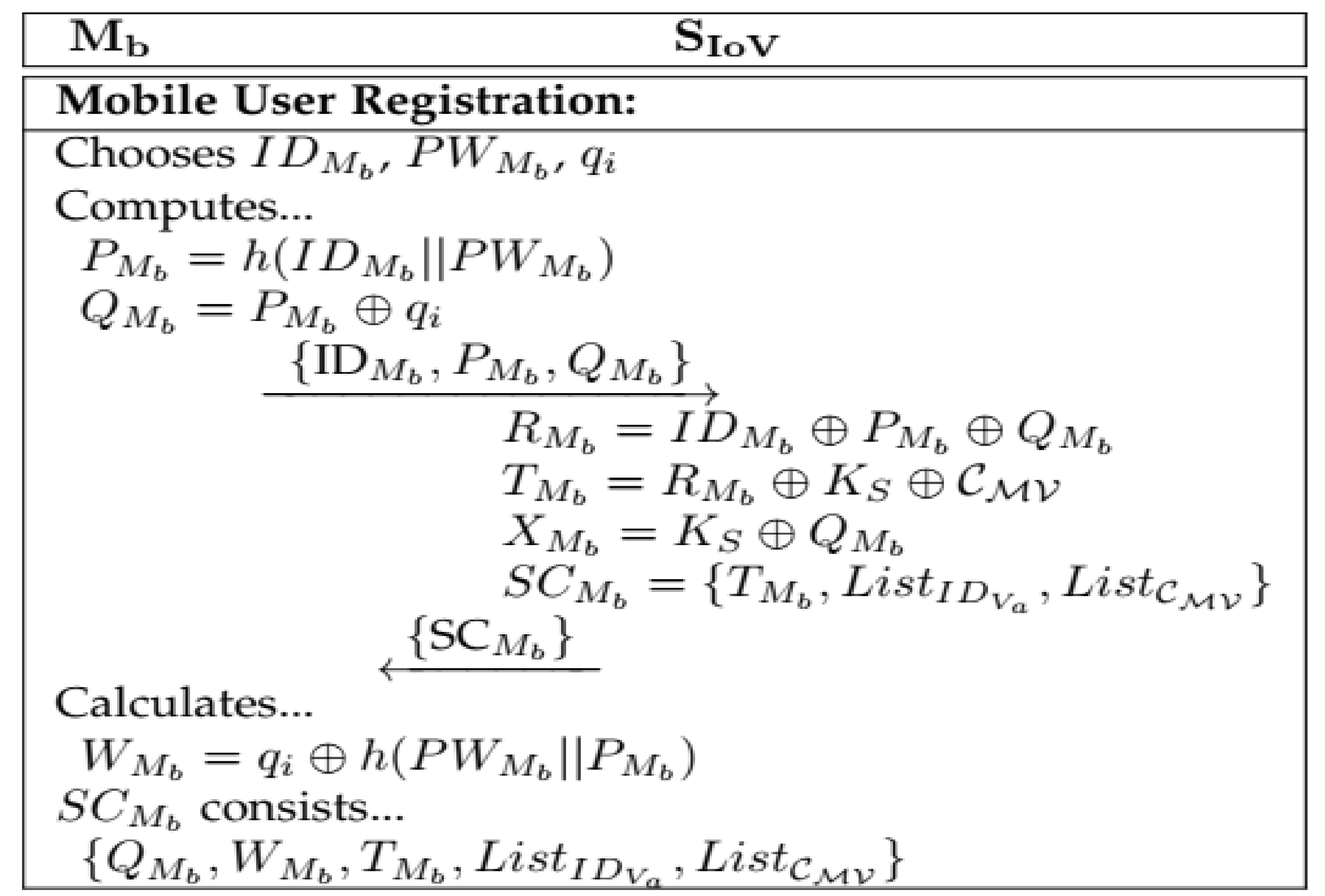
$$\xleftarrow{\{\mathrm{TPD}_{V_a}\}}$$

Calculates...

$W_{V_a} = p_i \oplus h(PW_{V_a} || P_{V_a})$

Saves Q_{V_a}, W_{V_a} in TPD_{V_a}

IoVCom: Mobile User Registration Phase



$\mathbf{M_b}$	$\mathbf{S_{IoV}}$

Mobile User Registration:

Chooses ID_{M_b}, PW_{M_b}, q_i

Computes...

$P_{M_b} = h(ID_{M_b} || PW_{M_b})$

$Q_{M_b} = P_{M_b} \oplus q_i$

$\xrightarrow{\{\mathrm{ID}_{M_b}, P_{M_b}, Q_{M_b}\}}$

$R_{M_b} = ID_{M_b} \oplus P_{M_b} \oplus Q_{M_b}$

$T_{M_b} = R_{M_b} \oplus K_S \oplus \mathcal{C}_{\mathcal{MV}}$

$X_{M_b} = K_S \oplus Q_{M_b}$

$SC_{M_b} = \{T_{M_b}, List_{ID_{V_a}}, List_{\mathcal{C}_{\mathcal{MV}}}\}$

$\xleftarrow{\{\mathrm{SC}_{M_b}\}}$

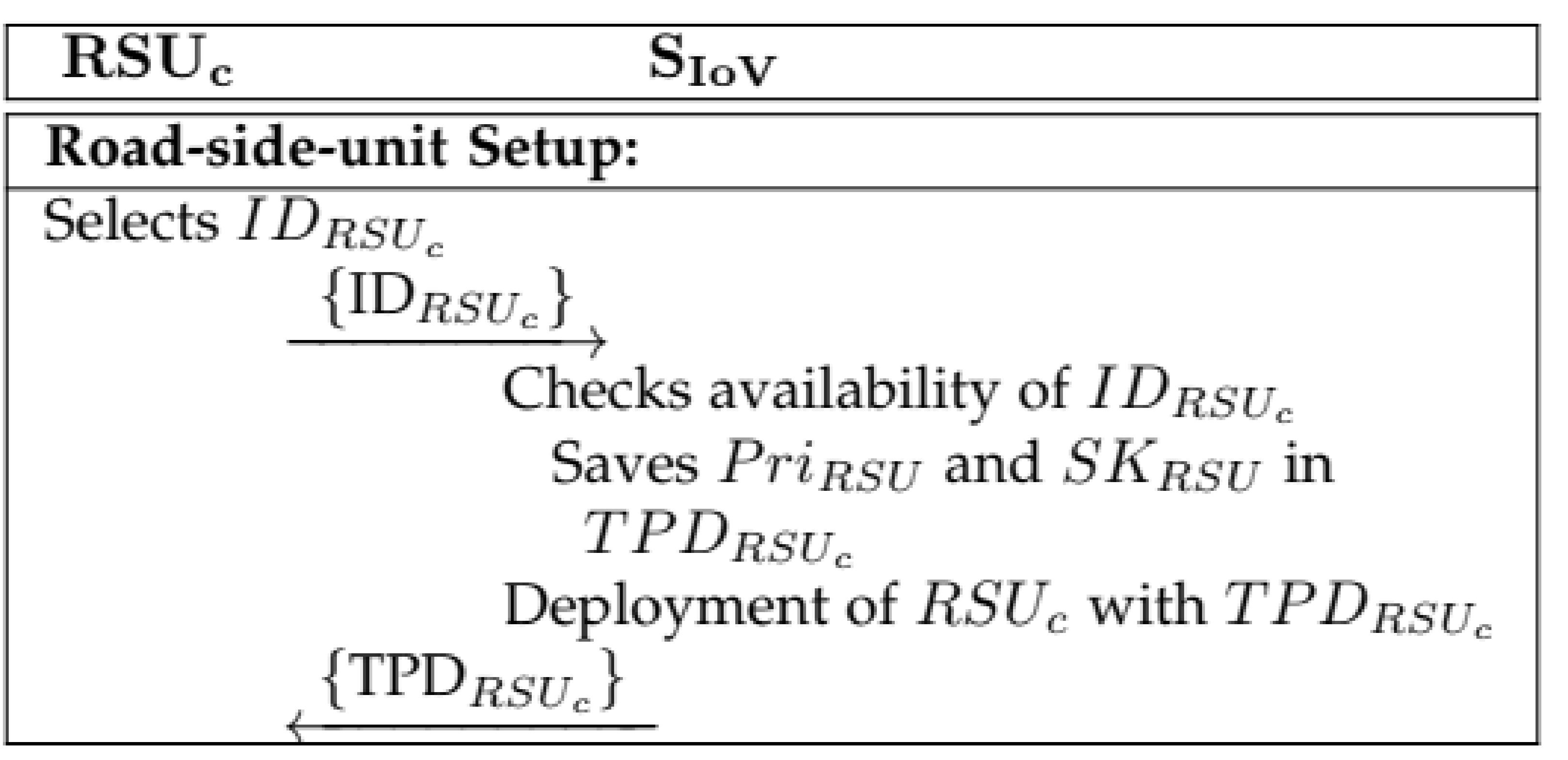
Calculates...

$W_{M_b} = q_i \oplus h(PW_{M_b} || P_{M_b})$

SC_{M_b} consists...

$\{Q_{M_b}, W_{M_b}, T_{M_b}, List_{ID_{V_a}}, List_{\mathcal{C}_{\mathcal{MV}}}\}$

IoVCom: Road-side-unit Setup



$\mathbf{RSU_c}$ $\mathbf{S_{IoV}}$

Road-side-unit Setup:

Selects ID_{RSU_c}

$\xrightarrow{\{\mathrm{ID}_{RSU_c}\}}$

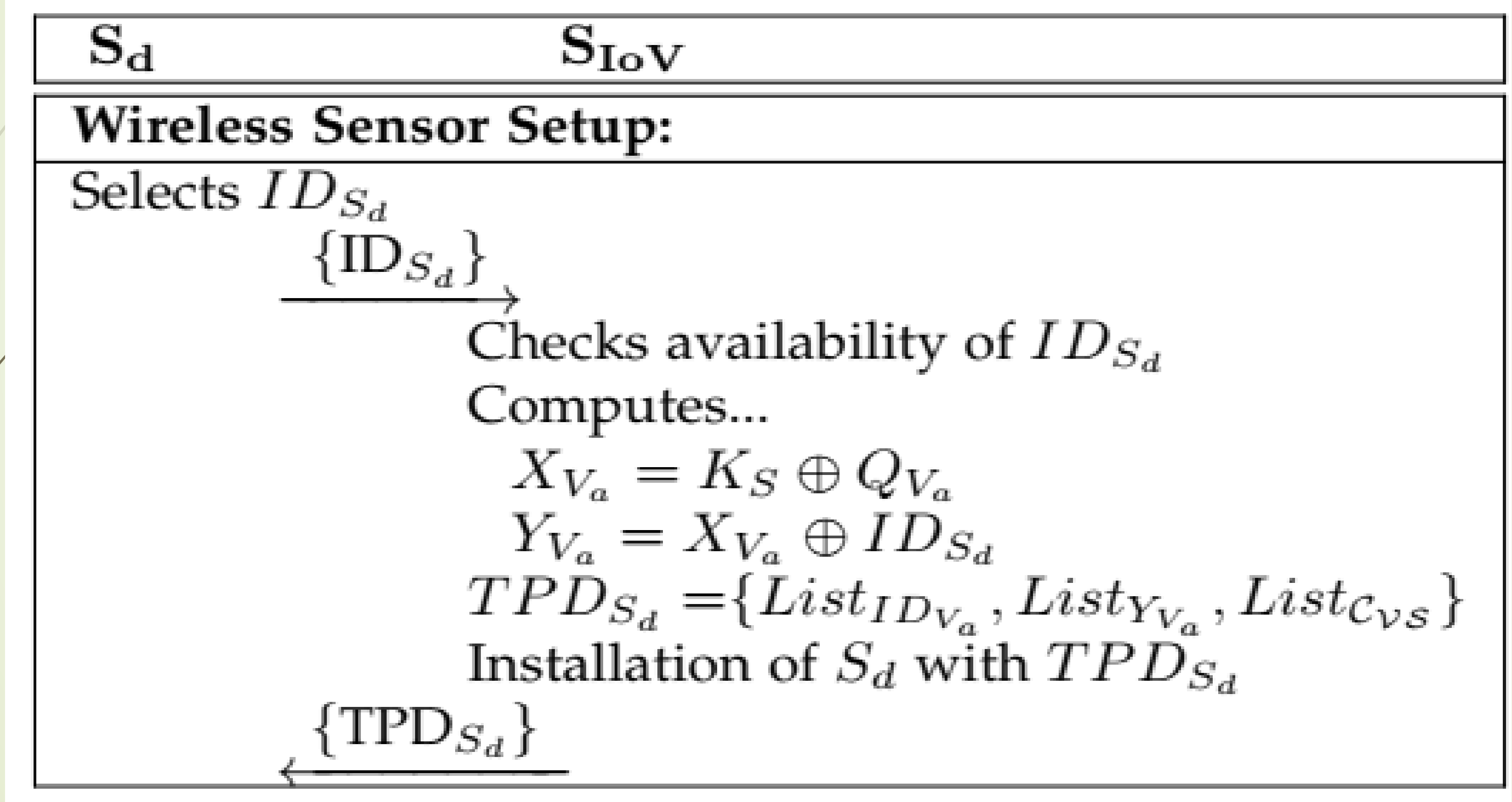
Checks availability of ID_{RSU_c}

Saves Pri_{RSU} and SK_{RSU} in TPD_{RSU_c}

Deployment of RSU_c with TPD_{RSU_c}

$\xleftarrow{\{\mathrm{TPD}_{RSU_c}\}}$

IoVCom: Wireless Sensor Setup



$\mathbf{S_d}$ $\mathbf{S_{IoV}}$

Wireless Sensor Setup:

Selects ID_{S_d}

$\xrightarrow{\{\mathrm{ID}_{S_d}\}}$

Checks availability of ID_{S_d}

Computes...

$X_{V_a} = K_S \oplus Q_{V_a}$

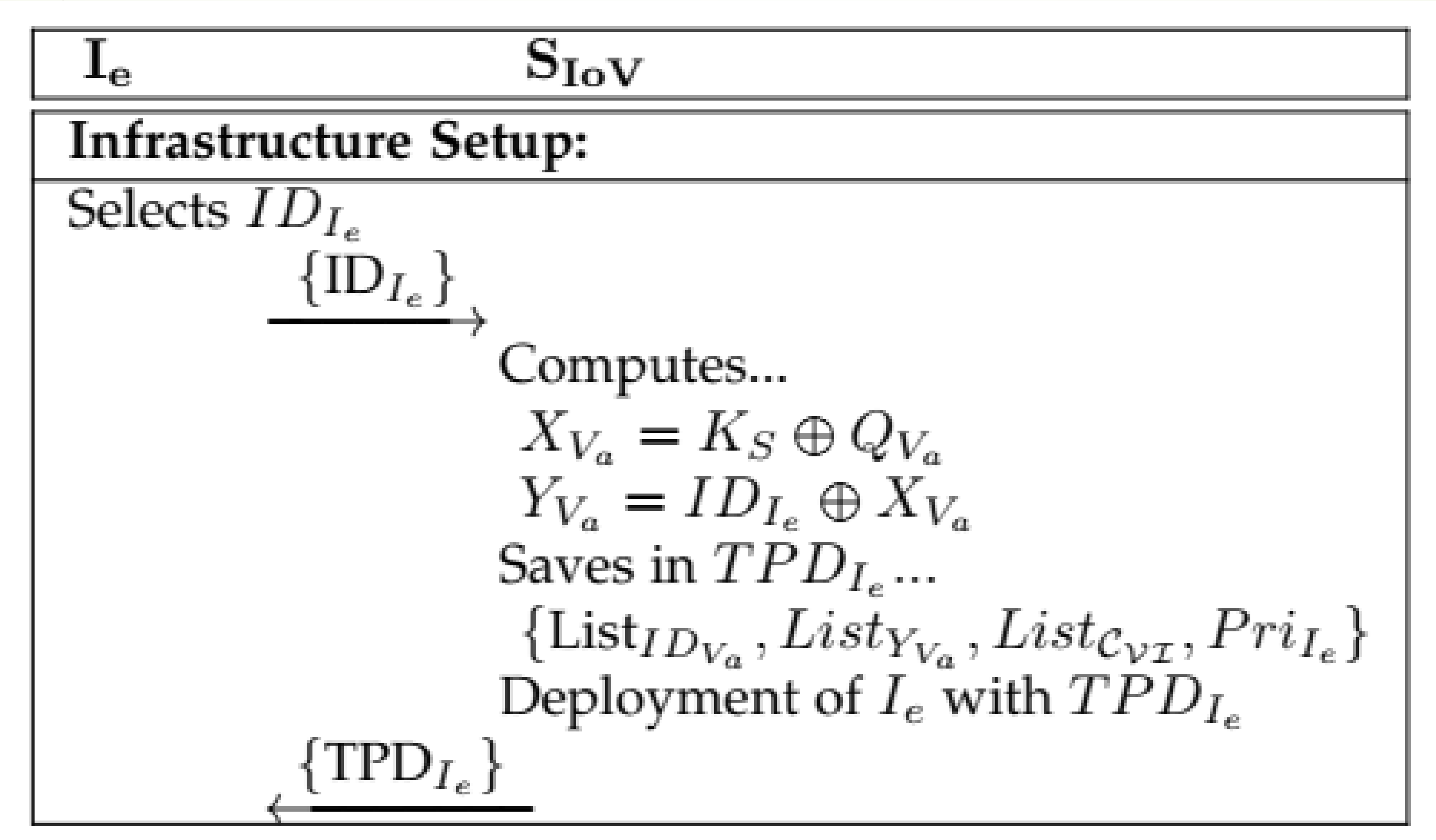
$Y_{V_a} = X_{V_a} \oplus ID_{S_d}$

$TPD_{S_d} =\{List_{ID_{V_a}}, List_{Y_{V_a}}, List_{C_{VS}}\}$

Installation of S_d with TPD_{S_d}

$\xleftarrow{\{\mathrm{TPD}_{S_d}\}}$

Infrastructure Setup



$\mathbf{I_e}$ $\mathbf{S_{IoV}}$

Infrastructure Setup:

Selects ID_{I_e}

$\xrightarrow{\{\mathrm{ID}_{I_e}\}}$

Computes...

$X_{V_a} = K_S \oplus Q_{V_a}$

$Y_{V_a} = ID_{I_e} \oplus X_{V_a}$

Saves in TPD_{I_e}...

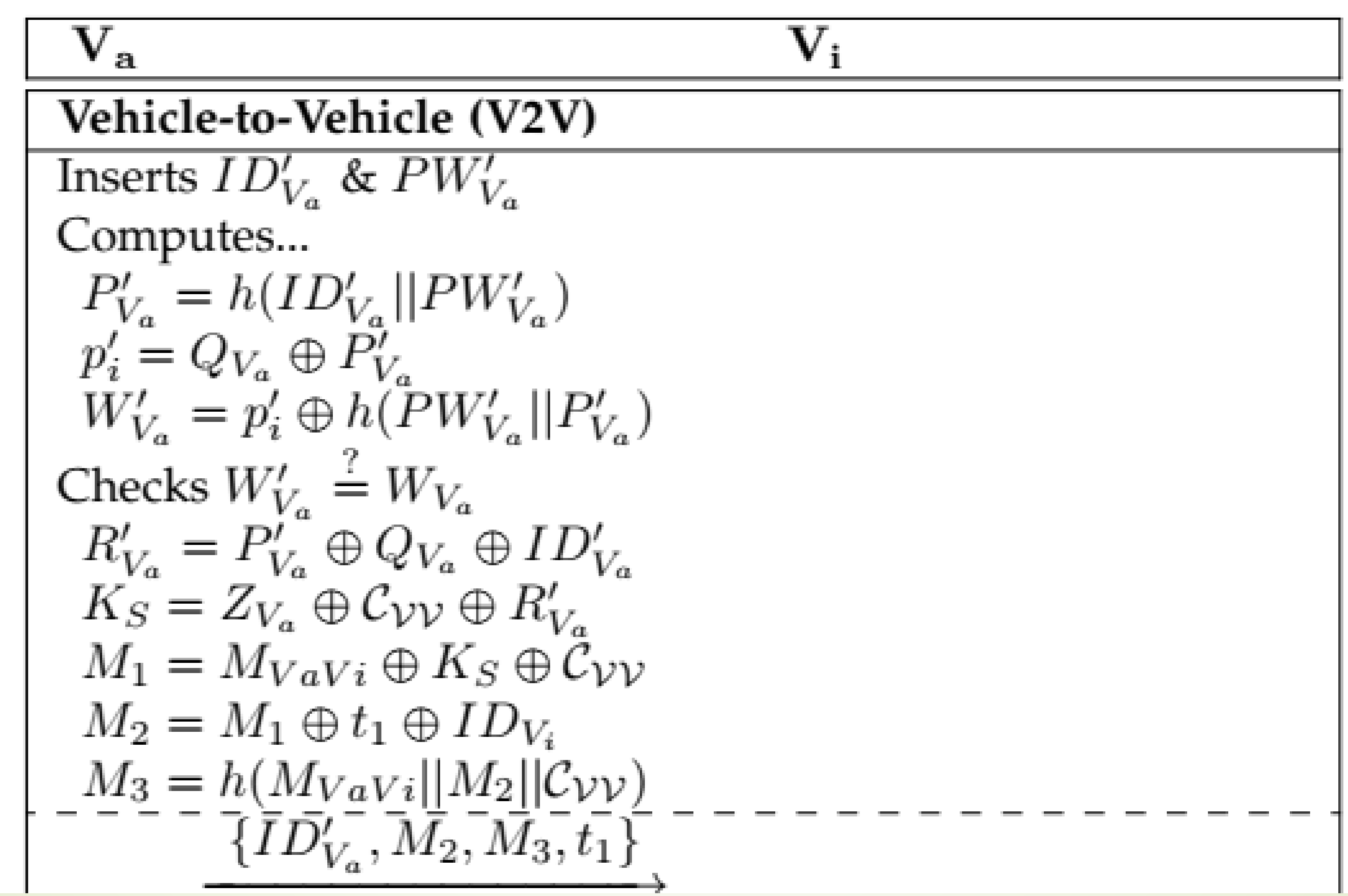
$\{\mathrm{List}_{ID_{V_a}}, List_{Y_{V_a}}, List_{\mathcal{C}_{V\mathcal{I}}}, Pri_{I_e}\}$

Deployment of I_e with TPD_{I_e}

$\xleftarrow{\{\mathrm{TPD}_{I_e}\}}$

The IoVCom: Data Transmission Schemes

Vehicle-to-Vehicle Data Transmission Schemes



$\mathbf{V_a}$	$\mathbf{V_i}$

Vehicle-to-Vehicle (V2V)

Inserts ID'_{V_a} & PW'_{V_a}

Computes...

$P'_{V_a} = h(ID'_{V_a}||PW'_{V_a})$

$p'_i = Q_{V_a} \oplus P'_{V_a}$

$W'_{V_a} = p'_i \oplus h(PW'_{V_a}||P'_{V_a})$

Checks $W'_{V_a} \overset{?}{=} W_{V_a}$

$R'_{V_a} = P'_{V_a} \oplus Q_{V_a} \oplus ID'_{V_a}$

$K_S = Z_{V_a} \oplus \mathcal{C}_{\mathcal{VV}} \oplus R'_{V_a}$

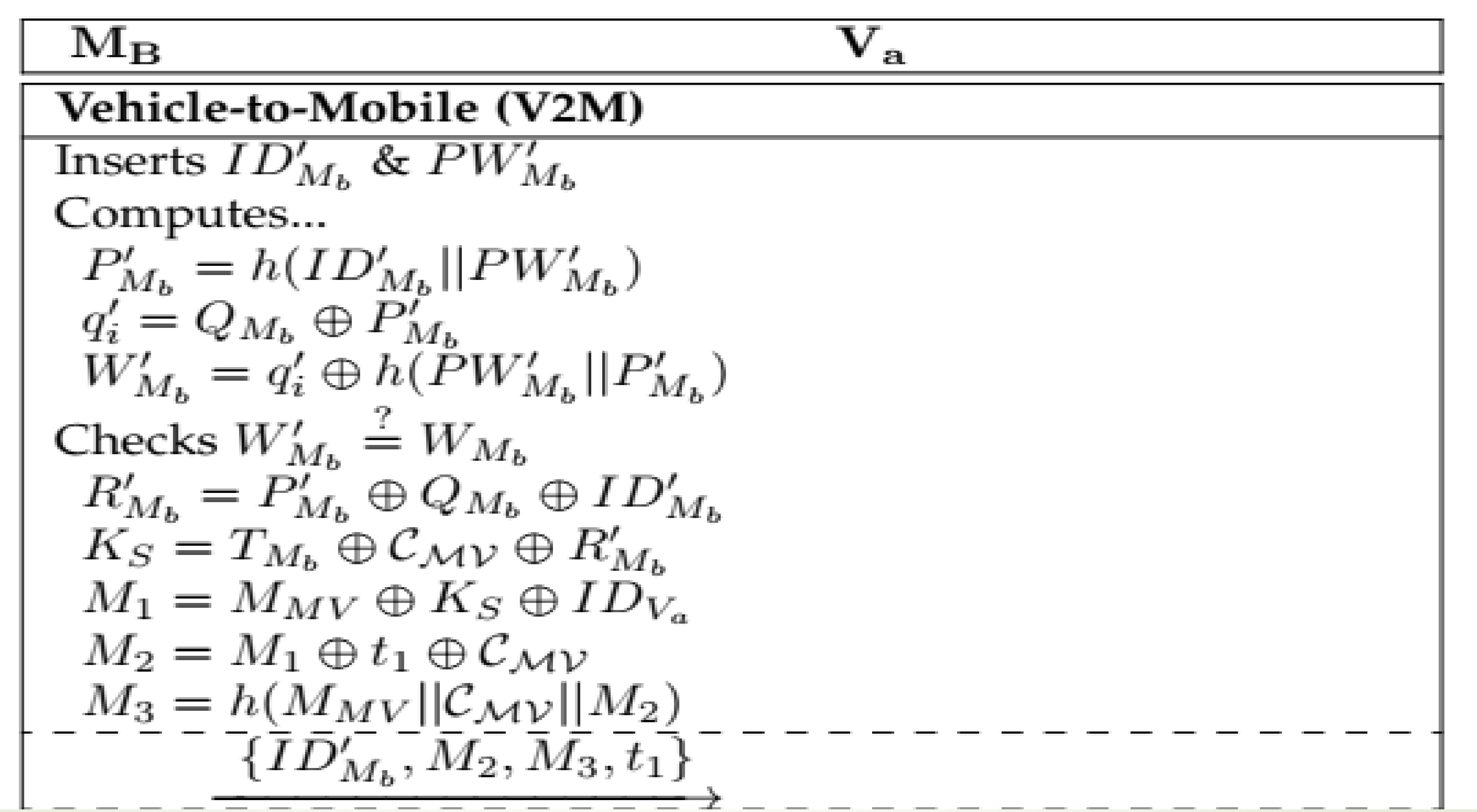
$M_1 = M_{VaVi} \oplus K_S \oplus \mathcal{C}_{\mathcal{VV}}$

$M_2 = M_1 \oplus t_1 \oplus ID_{V_i}$

$M_3 = h(M_{VaVi}||M_2||\mathcal{C}_{\mathcal{VV}})$

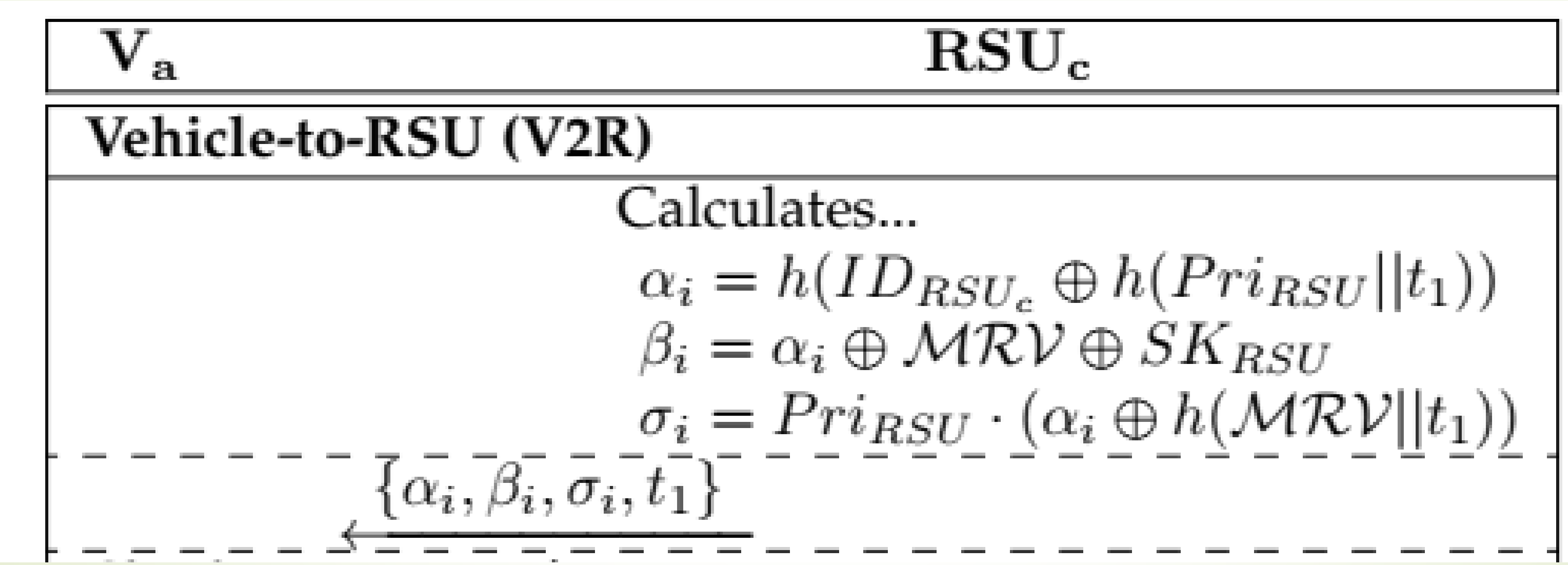
$$\xrightarrow{\{ID'_{V_a}, M_2, M_3, t_1\}}$$

IoVCom: V2M Communication



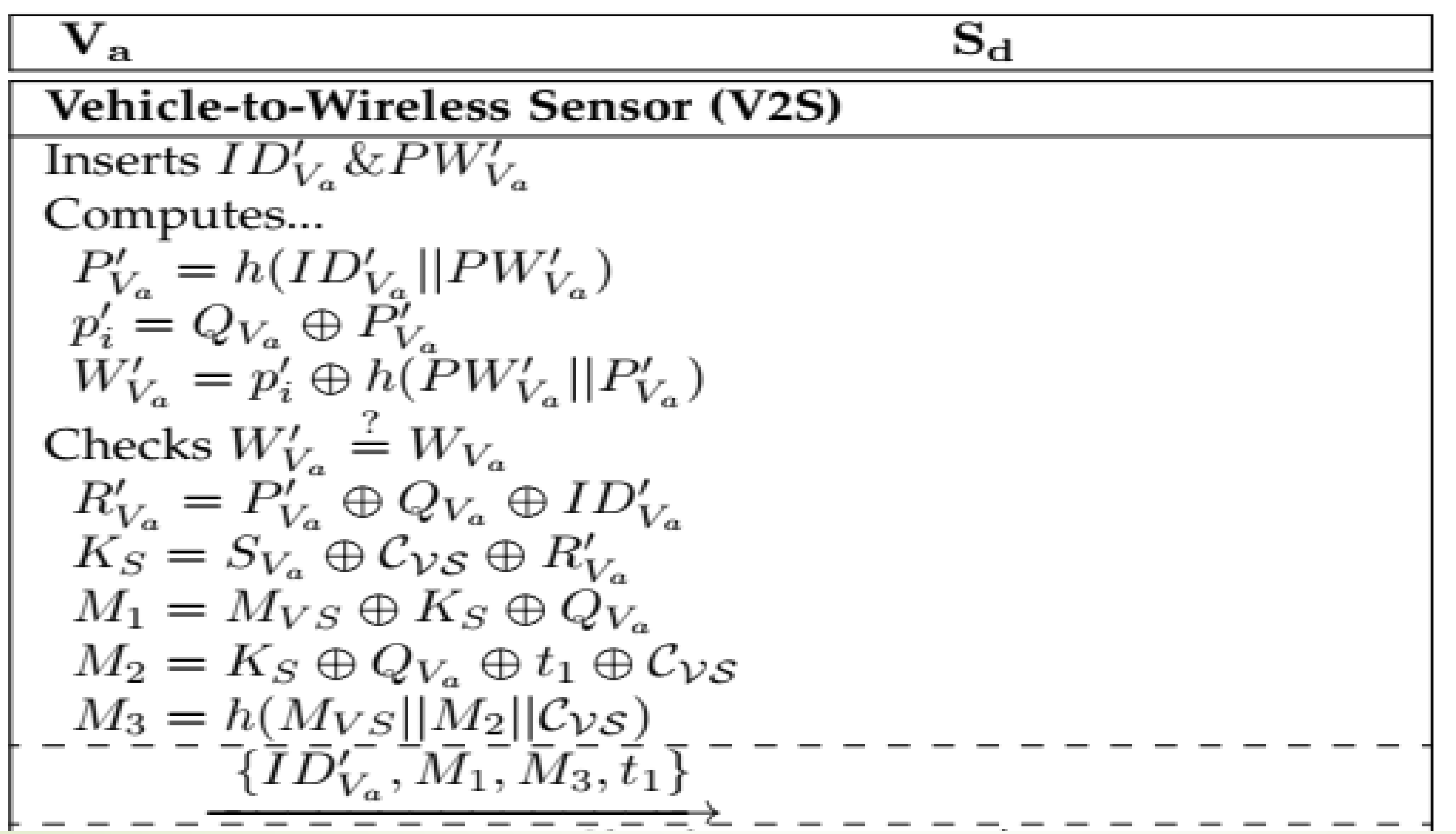
$\mathbf{M_B}$	$\mathbf{V_a}$
Vehicle-to-Mobile (V2M)	
Inserts ID'_{M_b} & PW'_{M_b}	
Computes...	
$P'_{M_b} = h(ID'_{M_b}\|\|PW'_{M_b})$	
$q'_i = Q_{M_b} \oplus P'_{M_b}$	
$W'_{M_b} = q'_i \oplus h(PW'_{M_b}\|\|P'_{M_b})$	
Checks $W'_{M_b} \overset{?}{=} W_{M_b}$	
$R'_{M_b} = P'_{M_b} \oplus Q_{M_b} \oplus ID'_{M_b}$	
$K_S = T_{M_b} \oplus \mathcal{C}_{\mathcal{MV}} \oplus R'_{M_b}$	
$M_1 = M_{MV} \oplus K_S \oplus ID_{V_a}$	
$M_2 = M_1 \oplus t_1 \oplus \mathcal{C}_{\mathcal{MV}}$	
$M_3 = h(M_{MV}\|\|\mathcal{C}_{\mathcal{MV}}\|\|M_2)$	
$\xrightarrow{\{ID'_{M_b}, M_2, M_3, t_1\}}$	

IoVCom: V2R Communication



$\mathbf{V_a}$	$\mathbf{RSU_c}$
Vehicle-to-RSU (V2R)	
	Calculates... $\alpha_i = h(ID_{RSU_c} \oplus h(Pri_{RSU} \| t_1))$ $\beta_i = \alpha_i \oplus \mathcal{MRV} \oplus SK_{RSU}$ $\sigma_i = Pri_{RSU} \cdot (\alpha_i \oplus h(\mathcal{MRV} \| t_1))$
$\xleftarrow{\{\alpha_i, \beta_i, \sigma_i, t_1\}}$	

IoVCom: V2S Communication



$\mathbf{V_a}$	$\mathbf{S_d}$

Vehicle-to-Wireless Sensor (V2S)

Inserts $ID'_{V_a} \& PW'_{V_a}$

Computes...

$P'_{V_a} = h(ID'_{V_a}||PW'_{V_a})$

$p'_i = Q_{V_a} \oplus P'_{V_a}$

$W'_{V_a} = p'_i \oplus h(PW'_{V_a}||P'_{V_a})$

Checks $W'_{V_a} \overset{?}{=} W_{V_a}$

$R'_{V_a} = P'_{V_a} \oplus Q_{V_a} \oplus ID'_{V_a}$

$K_S = S_{V_a} \oplus \mathcal{C}_{VS} \oplus R'_{V_a}$

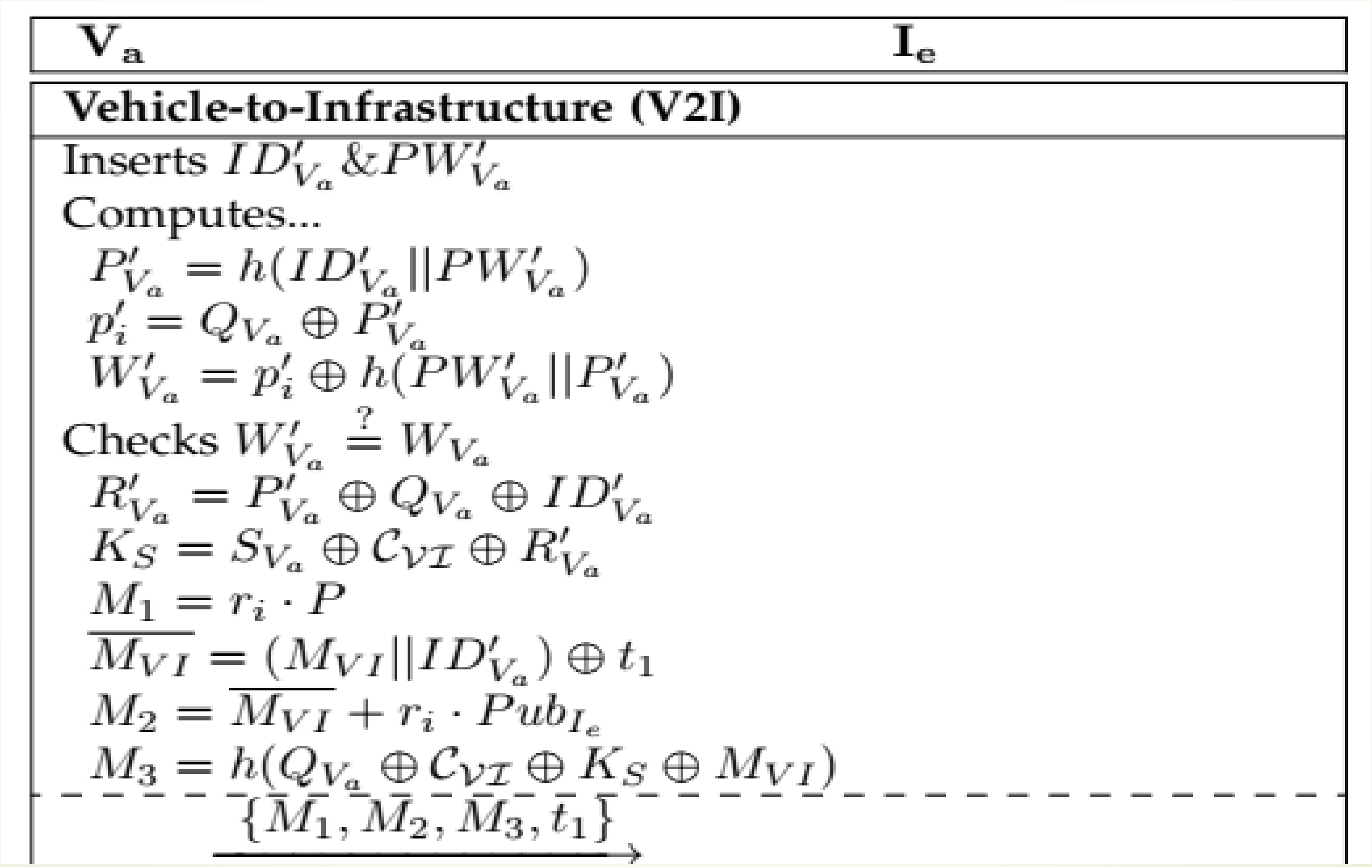
$M_1 = M_{VS} \oplus K_S \oplus Q_{V_a}$

$M_2 = K_S \oplus Q_{V_a} \oplus t_1 \oplus \mathcal{C}_{VS}$

$M_3 = h(M_{VS}||M_2||\mathcal{C}_{VS})$

$\xrightarrow{\{ID'_{V_a}, M_1, M_3, t_1\}}$

IoVCom: V2I Communication



$\mathbf{V_a}$ **$\mathbf{I_e}$**

Vehicle-to-Infrastructure (V2I)

Inserts $ID'_{V_a} \& PW'_{V_a}$

Computes...

$P'_{V_a} = h(ID'_{V_a} || PW'_{V_a})$

$p'_i = Q_{V_a} \oplus P'_{V_a}$

$W'_{V_a} = p'_i \oplus h(PW'_{V_a} || P'_{V_a})$

Checks $W'_{V_a} \overset{?}{=} W_{V_a}$

$R'_{V_a} = P'_{V_a} \oplus Q_{V_a} \oplus ID'_{V_a}$

$K_S = S_{V_a} \oplus \mathcal{C}_{\mathcal{VI}} \oplus R'_{V_a}$

$M_1 = r_i \cdot P$

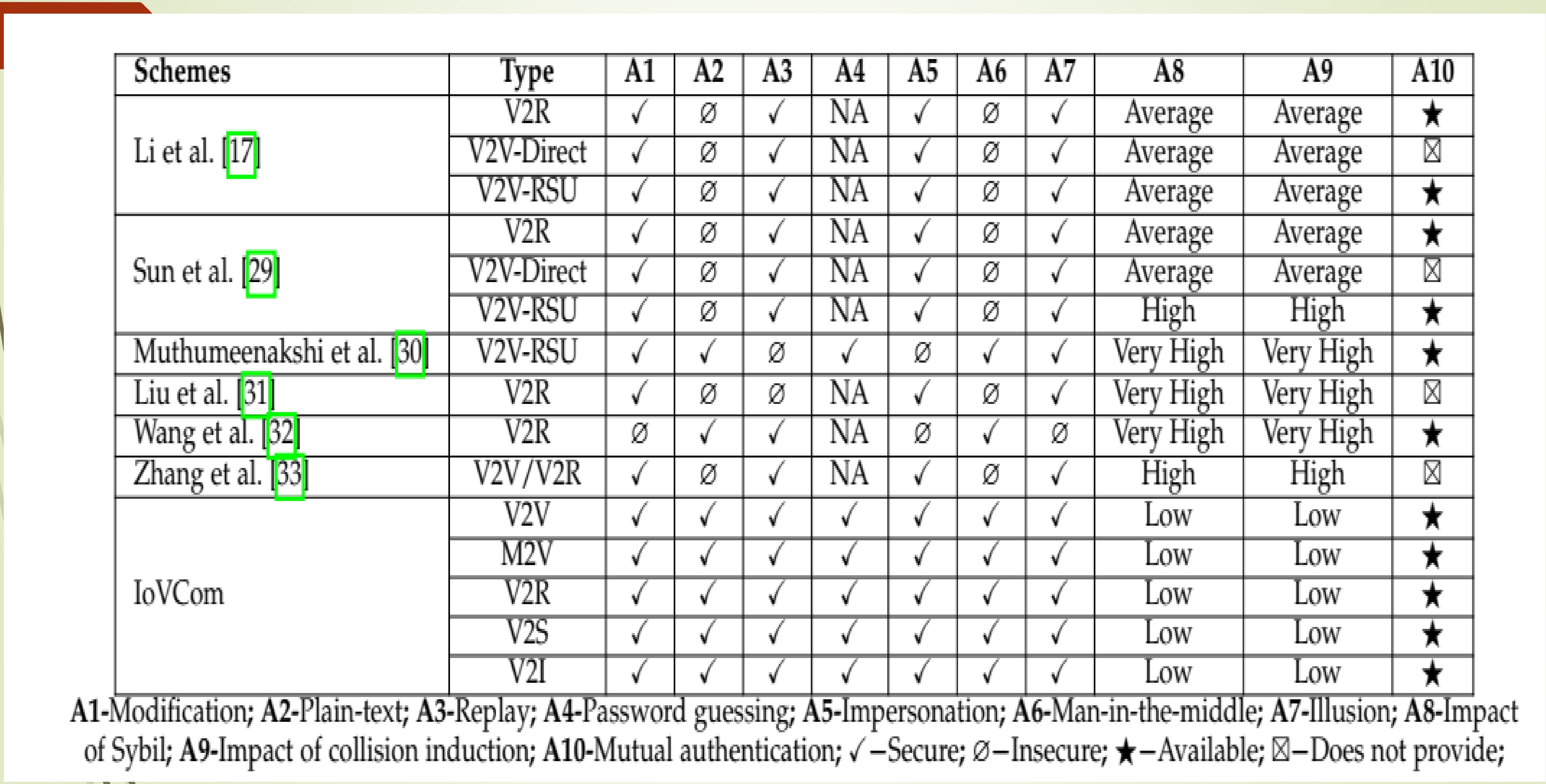
$\overline{M_{VI}} = (M_{VI} || ID'_{V_a}) \oplus t_1$

$M_2 = \overline{M_{VI}} + r_i \cdot Pub_{I_e}$

$M_3 = h(Q_{V_a} \oplus \mathcal{C}_{\mathcal{VI}} \oplus K_S \oplus M_{VI})$

$\xrightarrow{\{M_1, M_2, M_3, t_1\}}$

Security Attributes Comparison for Relevant Vehicular Communication Schemes



Schemes	Type	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10
Li et al. [17]	V2R	✓	∅	✓	NA	✓	∅	✓	Average	Average	★
	V2V-Direct	✓	∅	✓	NA	✓	∅	✓	Average	Average	☒
	V2V-RSU	✓	∅	✓	NA	✓	∅	✓	Average	Average	★
Sun et al. [29]	V2R	✓	∅	✓	NA	✓	∅	✓	Average	Average	★
	V2V-Direct	✓	∅	✓	NA	✓	∅	✓	Average	Average	☒
	V2V-RSU	✓	∅	✓	NA	✓	∅	✓	High	High	★
Muthumeenakshi et al. [30]	V2V-RSU	✓	✓	∅	✓	∅	✓	✓	Very High	Very High	★
Liu et al. [31]	V2R	✓	∅	∅	NA	✓	∅	✓	Very High	Very High	☒
Wang et al. [32]	V2R	∅	✓	✓	NA	∅	✓	∅	Very High	Very High	★
Zhang et al. [33]	V2V/V2R	✓	∅	✓	NA	✓	∅	✓	High	High	☒
IoVCom	V2V	✓	✓	✓	✓	✓	✓	✓	Low	Low	★
	M2V	✓	✓	✓	✓	✓	✓	✓	Low	Low	★
	V2R	✓	✓	✓	✓	✓	✓	✓	Low	Low	★
	V2S	✓	✓	✓	✓	✓	✓	✓	Low	Low	★
	V2I	✓	✓	✓	✓	✓	✓	✓	Low	Low	★

A1-Modification; **A2**-Plain-text; **A3**-Replay; **A4**-Password guessing; **A5**-Impersonation; **A6**-Man-in-the-middle; **A7**-Illusion; **A8**-Impact of Sybil; **A9**-Impact of collision induction; **A10**-Mutual authentication; ✓–Secure; ∅–Insecure; ★–Available; ☒–Does not provide;

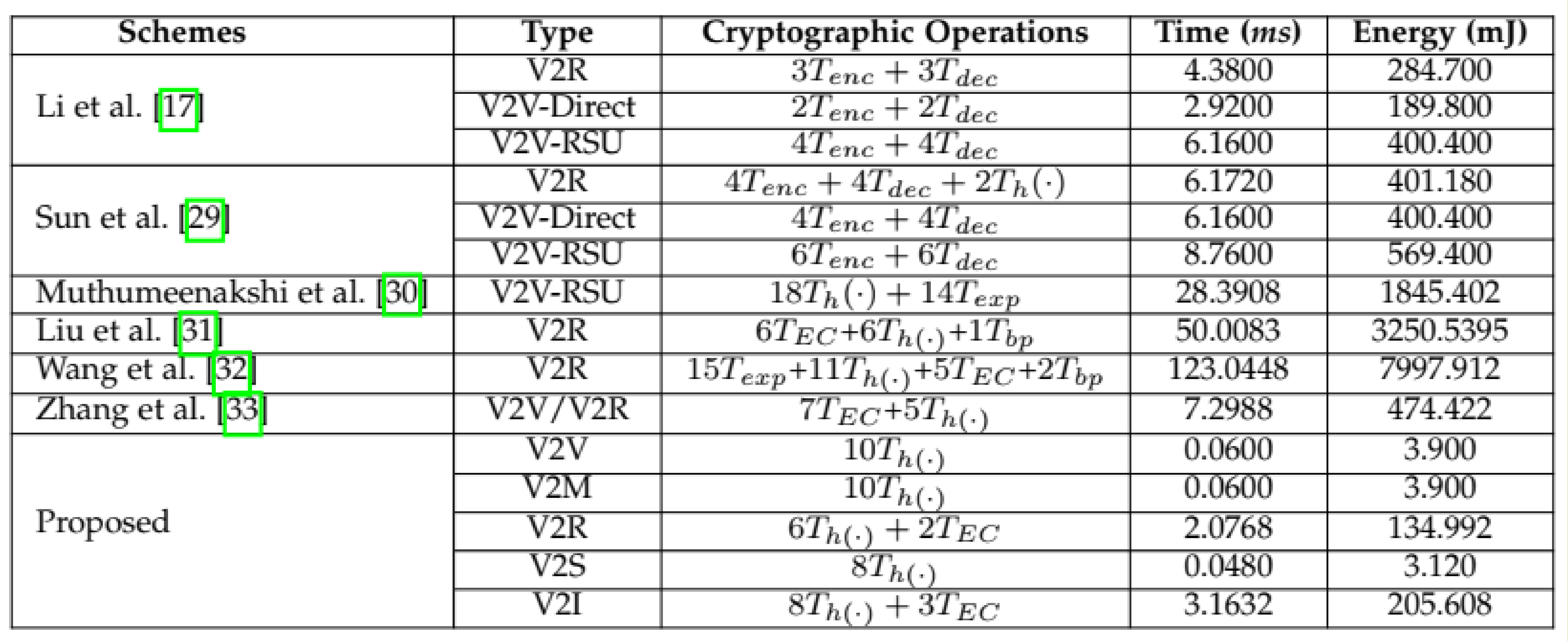
Performance Analysis

- Computational Time
- Communication and Storage Cost
- Energy consumption

Simulation Environment

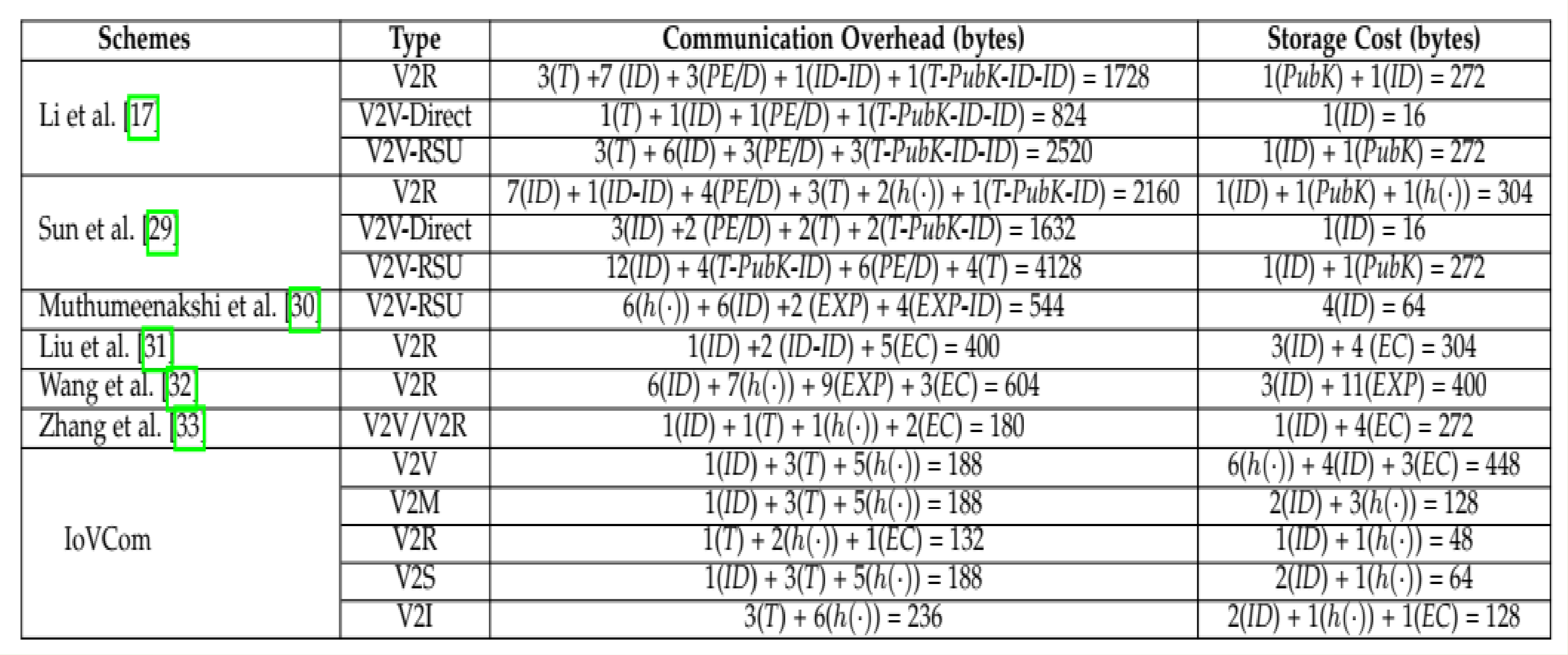
- Vehicular communication schemes are designed using different operations, **i.e., one-way hash function (Th(·)), asymmetric encryption/decryption (Tenc=Tdec), EC multiplication (TEC), exponential (Texp), and bi-linear pairing (Tbp).**
- On the system configuration **(Intel(R) Core (TM), 5200U 2.20 GHz, Core i5 processor, RAM 8 GB)**, **Th(·)** expects **0.0060 milliseconds (ms)** and **Texp needs 2.0202 ms**.
- Further, **Tenc requires 1.2861 ms, Tdec takes 38.9570 ms**, TEC needs 1.0384 ms, and **Tbp requires 43.7419 ms**.

Computational Analysis Statistics for Different Communication Protocols



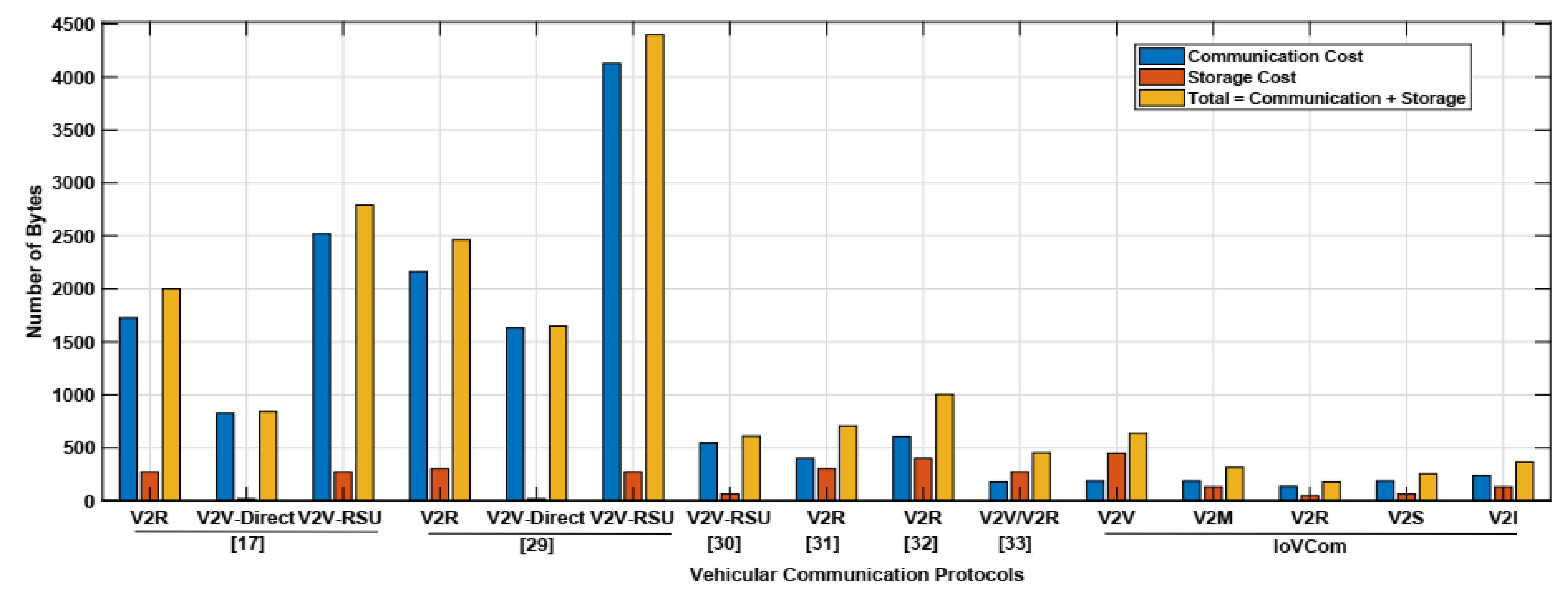
Schemes	Type	Cryptographic Operations	Time (ms)	Energy (mJ)
Li et al. [17]	V2R	$3T_{enc} + 3T_{dec}$	4.3800	284.700
	V2V-Direct	$2T_{enc} + 2T_{dec}$	2.9200	189.800
	V2V-RSU	$4T_{enc} + 4T_{dec}$	6.1600	400.400
Sun et al. [29]	V2R	$4T_{enc} + 4T_{dec} + 2T_h(\cdot)$	6.1720	401.180
	V2V-Direct	$4T_{enc} + 4T_{dec}$	6.1600	400.400
	V2V-RSU	$6T_{enc} + 6T_{dec}$	8.7600	569.400
Muthumeenakshi et al. [30]	V2V-RSU	$18T_h(\cdot) + 14T_{exp}$	28.3908	1845.402
Liu et al. [31]	V2R	$6T_{EC}+6T_{h(\cdot)}+1T_{bp}$	50.0083	3250.5395
Wang et al. [32]	V2R	$15T_{exp}+11T_{h(\cdot)}+5T_{EC}+2T_{bp}$	123.0448	7997.912
Zhang et al. [33]	V2V/V2R	$7T_{EC}+5T_{h(\cdot)}$	7.2988	474.422
Proposed	V2V	$10T_{h(\cdot)}$	0.0600	3.900
	V2M	$10T_{h(\cdot)}$	0.0600	3.900
	V2R	$6T_{h(\cdot)} + 2T_{EC}$	2.0768	134.992
	V2S	$8T_{h(\cdot)}$	0.0480	3.120
	V2I	$8T_{h(\cdot)} + 3T_{EC}$	3.1632	205.608

Communication and Storage Cost Comparison for Various Communication Protocols



Schemes	Type	Communication Overhead (bytes)	Storage Cost (bytes)
Li et al. [17]	V2R	3(T) +7 (ID) + 3(PE/D) + 1(ID-ID) + 1(T-PubK-ID-ID) = 1728	1(PubK) + 1(ID) = 272
	V2V-Direct	1(T) + 1(ID) + 1(PE/D) + 1(T-PubK-ID-ID) = 824	1(ID) = 16
	V2V-RSU	3(T) + 6(ID) + 3(PE/D) + 3(T-PubK-ID-ID) = 2520	1(ID) + 1(PubK) = 272
Sun et al. [29]	V2R	7(ID) + 1(ID-ID) + 4(PE/D) + 3(T) + 2(h(·)) + 1(T-PubK-ID) = 2160	1(ID) + 1(PubK) + 1(h(·)) = 304
	V2V-Direct	3(ID) +2 (PE/D) + 2(T) + 2(T-PubK-ID) = 1632	1(ID) = 16
	V2V-RSU	12(ID) + 4(T-PubK-ID) + 6(PE/D) + 4(T) = 4128	1(ID) + 1(PubK) = 272
Muthumeenakshi et al. [30]	V2V-RSU	6(h(·)) + 6(ID) +2 (EXP) + 4(EXP-ID) = 544	4(ID) = 64
Liu et al. [31]	V2R	1(ID) +2 (ID-ID) + 5(EC) = 400	3(ID) + 4 (EC) = 304
Wang et al. [32]	V2R	6(ID) + 7(h(·)) + 9(EXP) + 3(EC) = 604	3(ID) + 11(EXP) = 400
Zhang et al. [33]	V2V/V2R	1(ID) + 1(T) + 1(h(·)) + 2(EC) = 180	1(ID) + 4(EC) = 272
IoVCom	V2V	1(ID) + 3(T) + 5(h(·)) = 188	6(h(·)) + 4(ID) + 3(EC) = 448
	V2M	1(ID) + 3(T) + 5(h(·)) = 188	2(ID) + 3(h(·)) = 128
	V2R	1(T) + 2(h(·)) + 1(EC) = 132	1(ID) + 1(h(·)) = 48
	V2S	1(ID) + 3(T) + 5(h(·)) = 188	2(ID) + 1(h(·)) = 64
	V2I	3(T) + 6(h(·)) = 236	2(ID) + 1(h(·)) + 1(EC) = 128

Total (communication and storage) cost comparison for different vehicular communication schemes



Conclusions and Future Works

- We have proposed a secure and energy-efficient communication system for the IoV architecture by including all five communications (V2V, V2R, V2M, V2S, and V2I).
- Thus, the IoVCom is helpful in various applications for vehicle users on the road.
- Moreover, security evaluations show that the IoVCom resists to well-known security attacks such as Sybil, user impersonation, illusion, modification, collision induction, man-in-the-middle, password guessing, plain-text, and replay.
- We have compared the IoVCom with different communication protocols (of VANETs, IoT, and IoV) to measure performance (for storage cost, communication overhead, execution time, and energy consumption), and the performance results achieve better outcomes comparatively.

Conclusions and Future Works

- Hence, the IoVCom is highly expedient for IoVbased applications in this smart environment.
- Therefore, the proposed communication protocols can be practiced reliably in different smart city applications to transmit meaningful data between IoV components, **and this will generate a new source of revenue for private and public sector stakeholders**
- In the future, we shall come up with new communication protocols for the IoV framework to resist future **cyberattacks by verifying security strengths through security tools and improve performance results.**

THANK YOU