Introduction to Intelligent Vehicles
[11. Security]

Chung-Wei Lin

cwlin@csie.ntu.edu.tw

CSIE Department

National Taiwan University

Security-Aware Design and Analysis

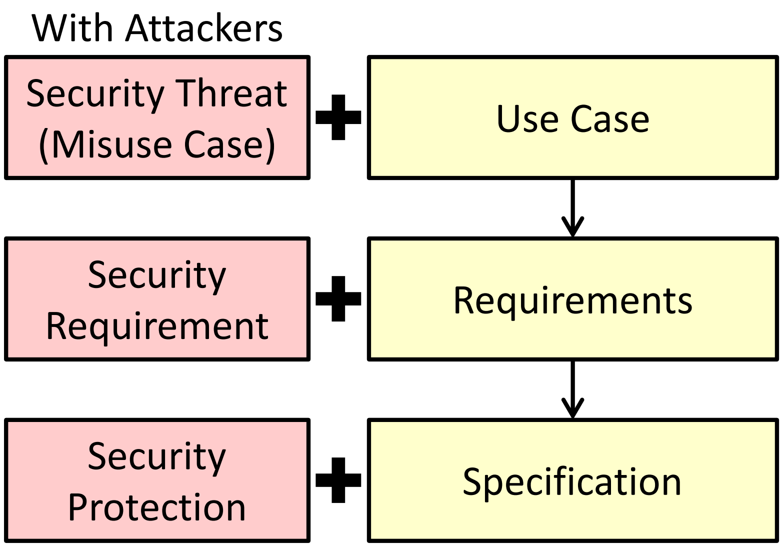
- Security is a rising concern, especially with connectivity

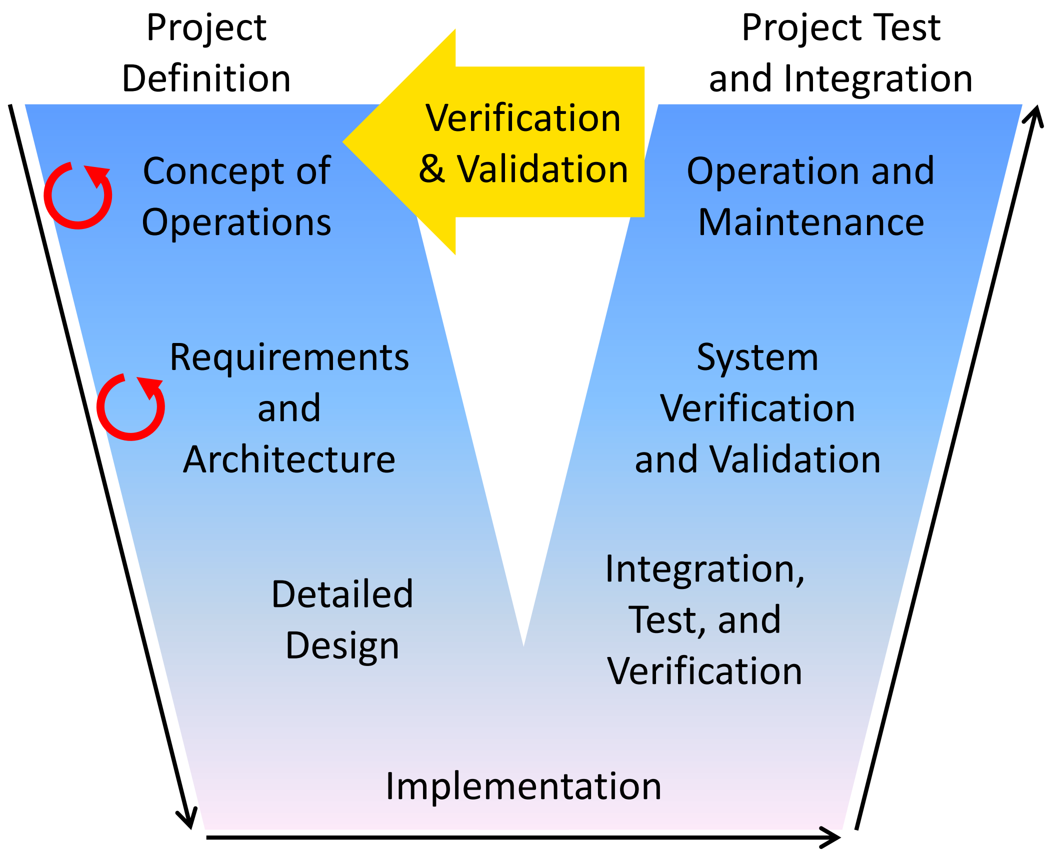
CBS News, Aug 19, 2014

Live Free or Die Hard (Movie), 2007

- One hypothetical (but very likely) scenario
  - Design stage
    - Use the RSA algorithm (strong and famous) for encryption, decryption, and authentication!
  - Implementation stage
    - Computing units on vehicles cannot afford it… (security mechanisms are usually computation-intensive)
  - Result: redesign systems (how can we prevent this?)

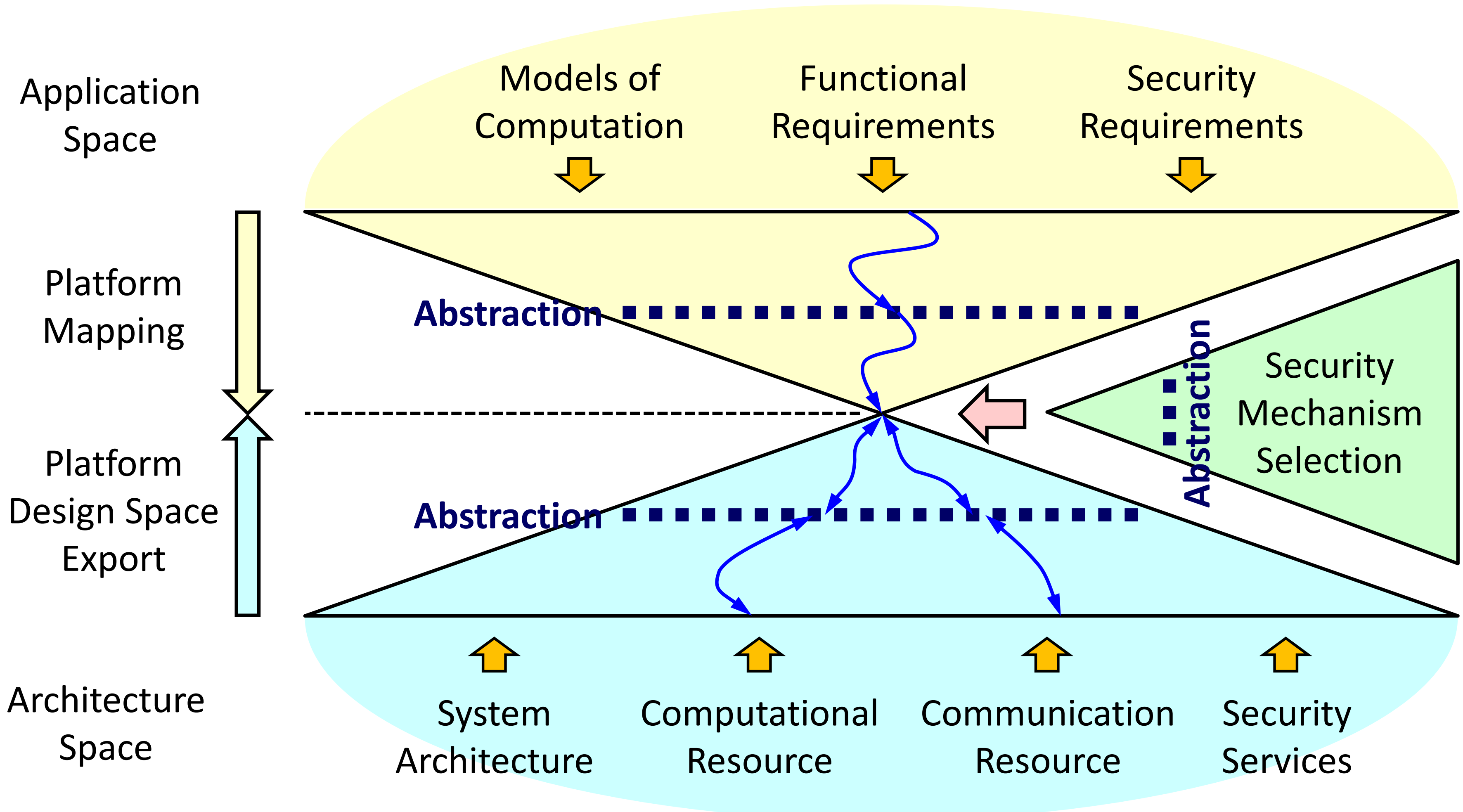
V Model with Security





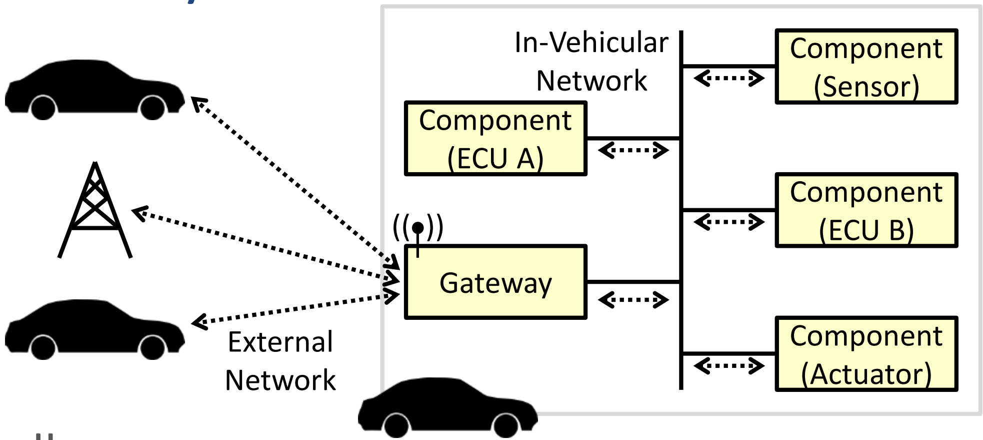
https://en.wikipedia.org/wiki/V-Model_(software_development)

Platform-Based Design with Security



Layered Security Protection

- Security requirements at each layer
  - **External network** with secure communication protocols integrated with existing standards and protocols such as DSRC
  - **Gateway** with intrusion detection systems and firewalls
  - **In-vehicular network** with lightweight authentication and encryption
  - **Component** with hardware security modules, secure boot, and secret key management



- Integrated formal languages or tools?
  - A simple tool: Microsoft Security Development Lifecycle (SDL) Threat Modeling Tool

Outline

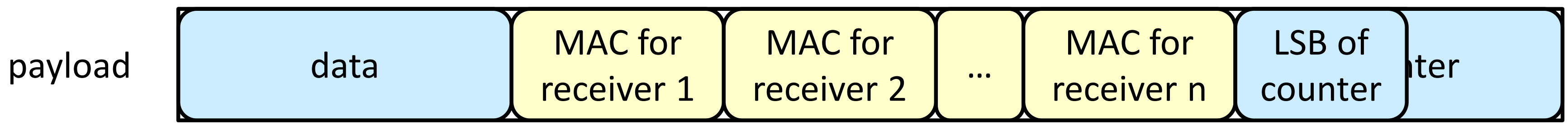
- **Message Authentication**
- Jamming Analysis
- Truthfulness Guarantee
- Intrusion Detection
- Consensus Algorithms
- Traffic Sign Design

Symmetric and Asymmetric Keys

- From Wikipedia
  - Symmetric-key algorithms for cryptography use the same cryptographic keys for both encryption of plaintext and decryption of ciphertext
  - Public-key cryptography (or asymmetric cryptography) uses pairs of keys
    - Public keys may be disseminated widely
    - Private keys are known only to the owner
- We are using symmetric keys until Slide 17

Message Authentication

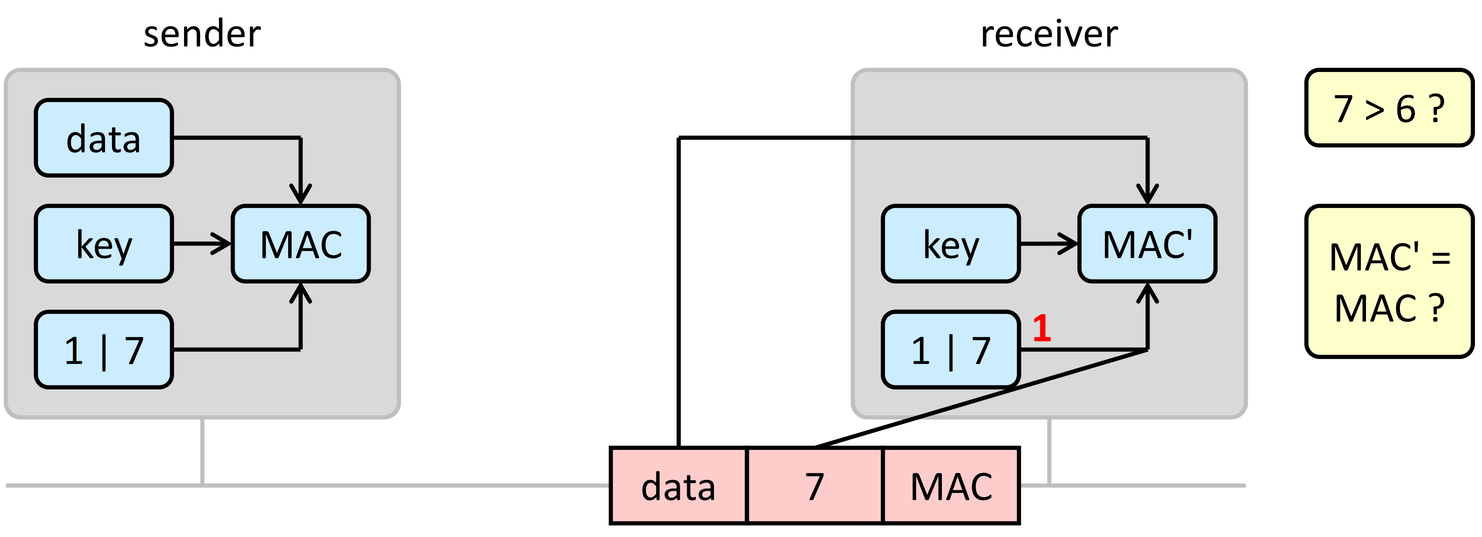
- A message is sent with MACs (Message Authentication Codes) to protect against **masquerade attacks**
  - Each receiver can authenticate it by checking if the corresponding MAC is equal to the MAC computed by itself
- A message is also sent with a counter to protect against **replay attacks**
  - Each receiver can check if the message is fresh or not



- Due to the limited size of the payload, only the least significant bits (LSBs) of the counter is sent with the message
  - Reset mechanisms are provided to avoid out-of-sync of counters

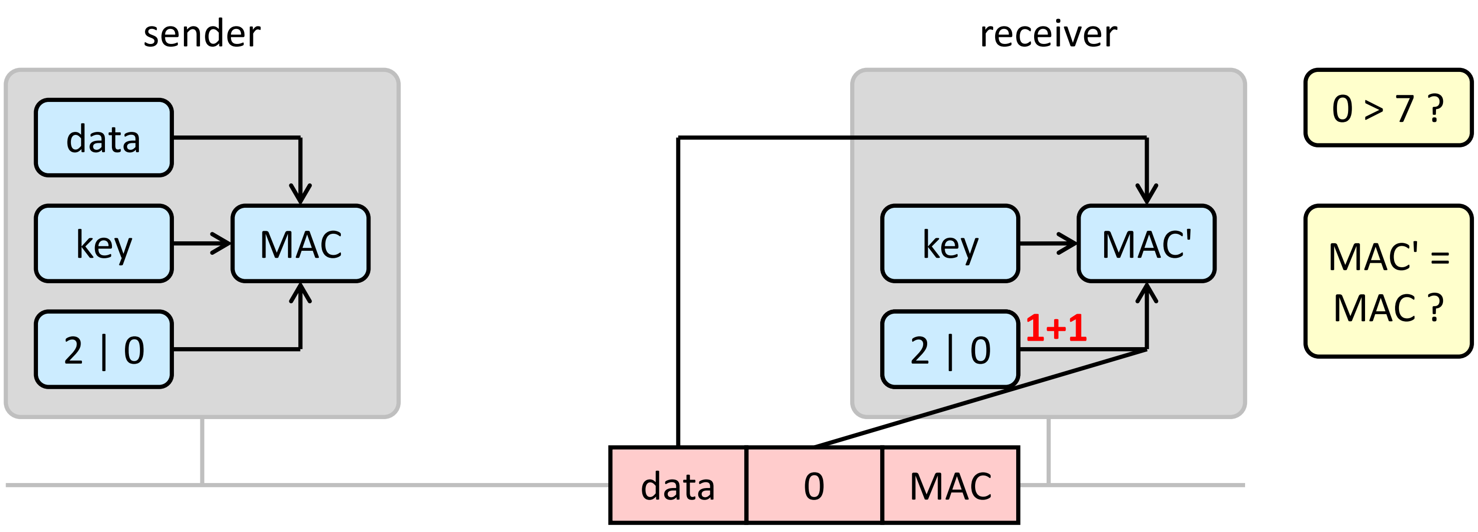
Sending Partial Counter

- We cannot afford to use many bits for the counter
  - There are only 64 bits for payload in CAN
- A counter C is divided into C_M and C_L
  - C_M: the most significant bits of C
  - C_L: the least significant bits of C
- Only C_L is sent!

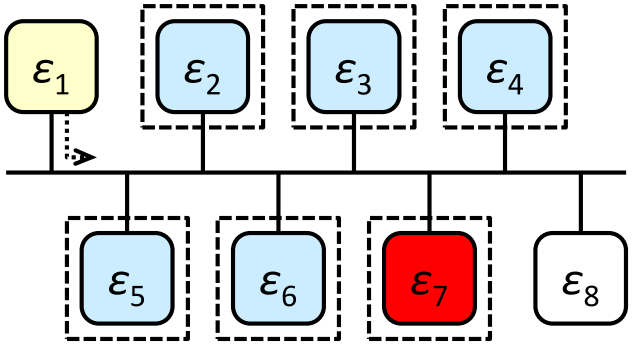


Sending Partial Counter

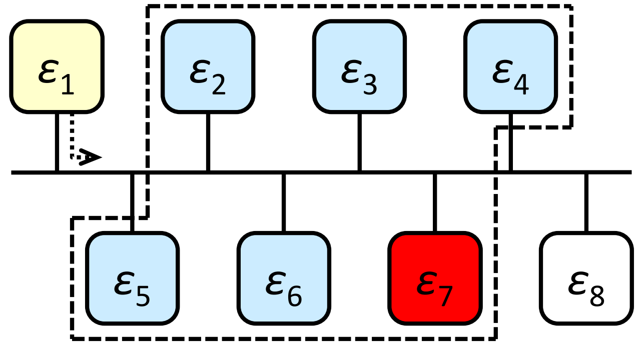
- We cannot afford to use many bits for the counter
  - There are only 64 bits for payload in CAN
- A counter C is divided into C_M and C_L
  - C_M: the most significant bits of C
  - C_L: the least significant bits of C
- Only C_L is sent!



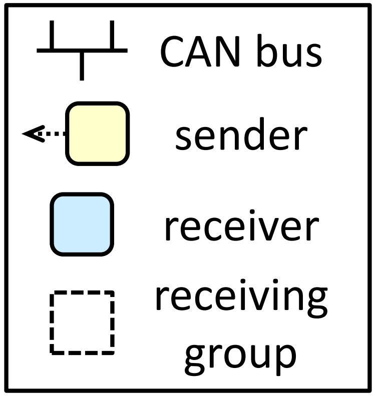
Spatial Key Management



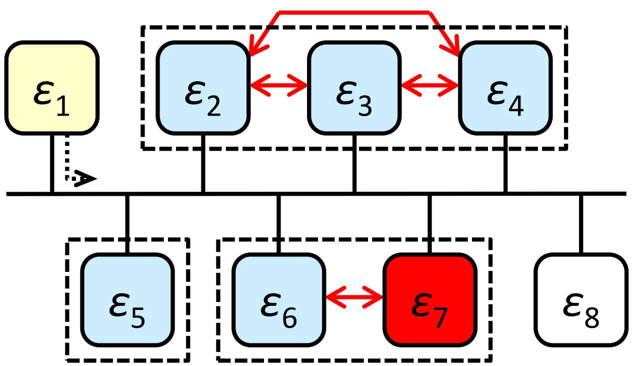
pair-wise key distribution



one-key-for-all key distribution



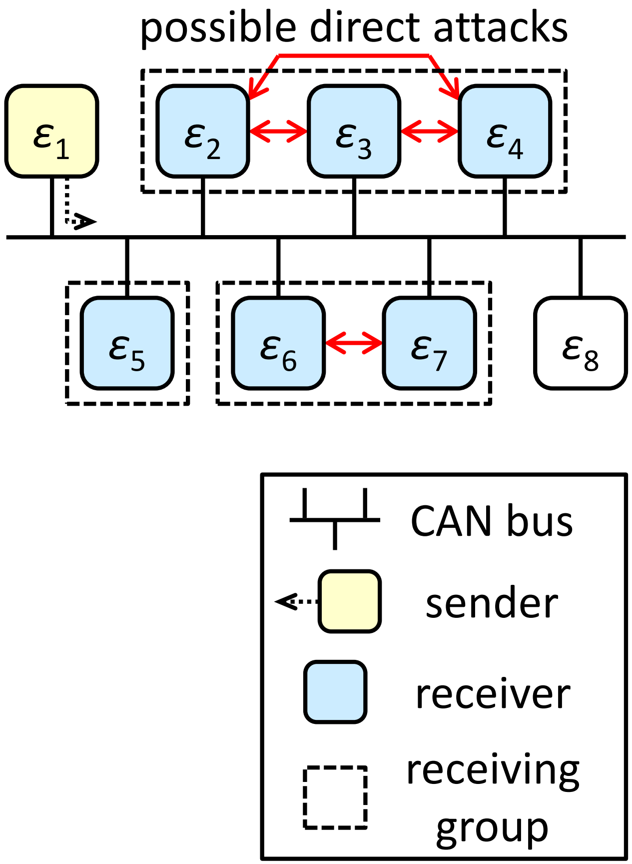
- ❑ Pair-wise key distribution
  - ➢ 6 MACs and no attack between receivers
- ❑ One-key-for-all key distribution
  - ➢ Only 1 MAC but attacks between receivers
- ❑ Tradeoff between security and bandwidth utilization



another key distribution

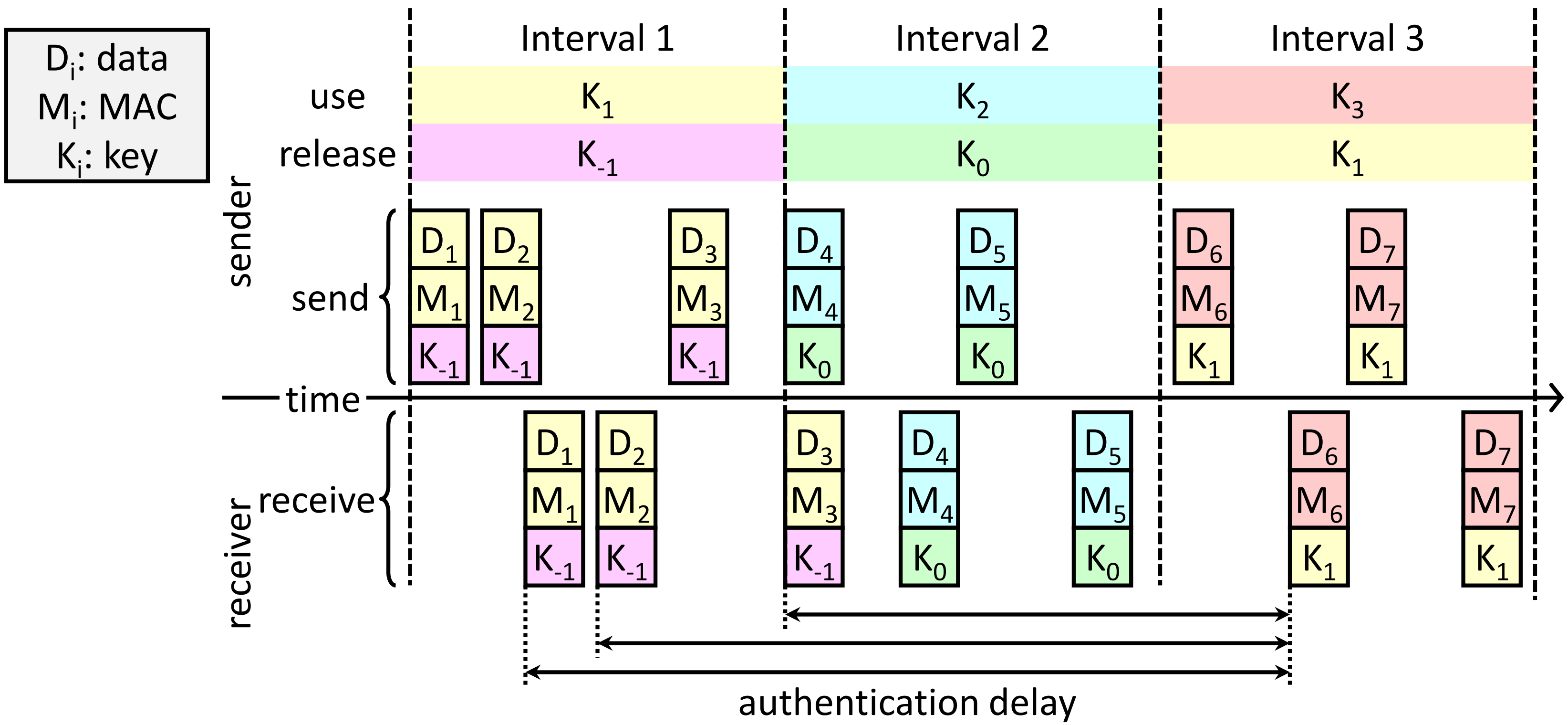
System Design

- For each signal σ, the total risk of direct attacks should be bounded
  - $R_{\sigma,2,3} + R_{\sigma,2,4} + R_{\sigma,3,4} + R_{\sigma,6,7} \le R_{\sigma}$
- For each receiver, the corresponding MAC length should be long enough
  - $L_2 \le L_{MAC1}$; $L_3 \le L_{MAC1}$; $L_4 \le L_{MAC1}$
  - $L_5 \le L_{MAC2}$
  - $L_6 \le L_{MAC3}$; $L_7 \le L_{MAC3}$
- The values of all R's and L's depend on
  - How critical a message is falsely accepted
  - How likely an existing ECU is compromised



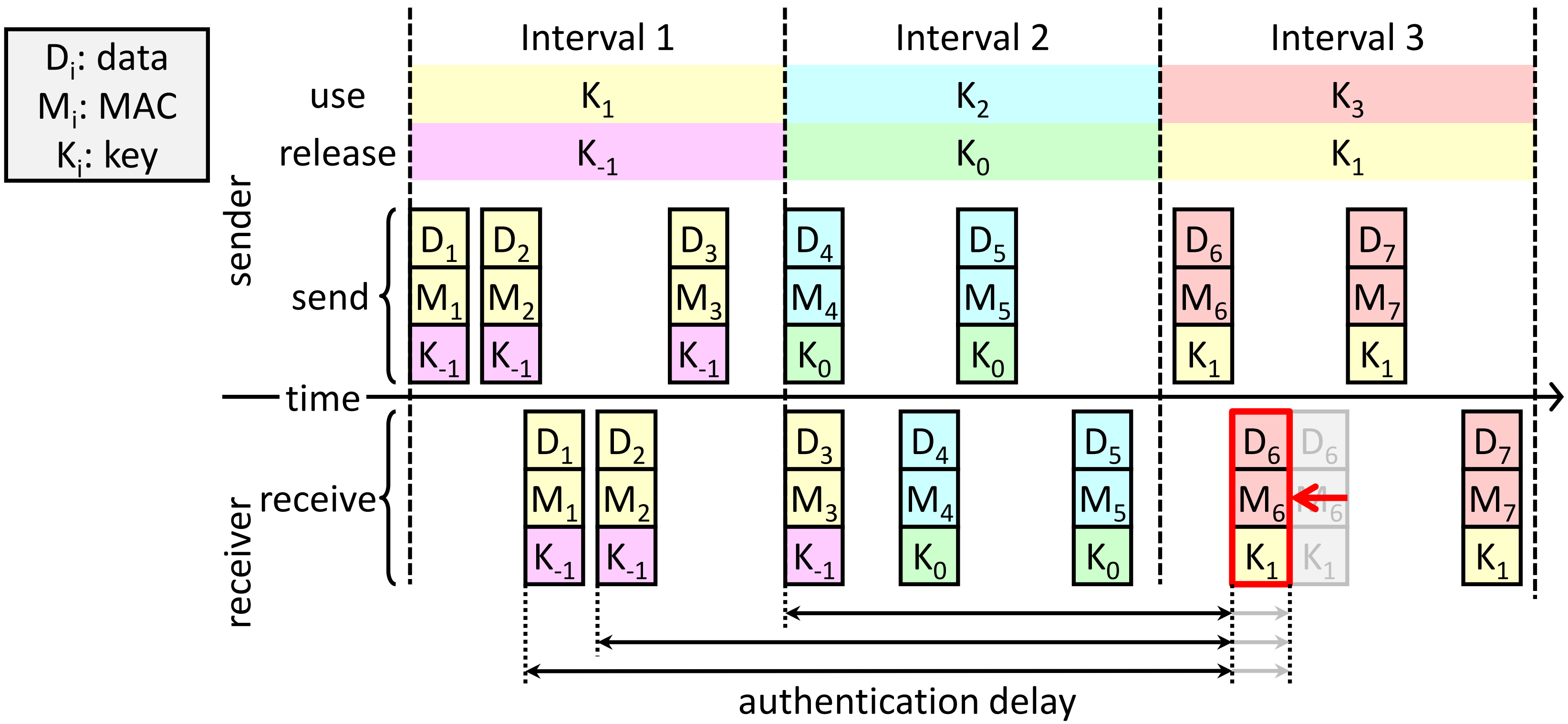
Temporal Key Management

- Timed Efficient Stream Loss-tolerant Authentication (TESLA) [Perrig et al.]
  - A sender sends data and MAC first and then releases the corresponding key later
  - A receiver stores data and MAC first and then checks them after receiving the corresponding key



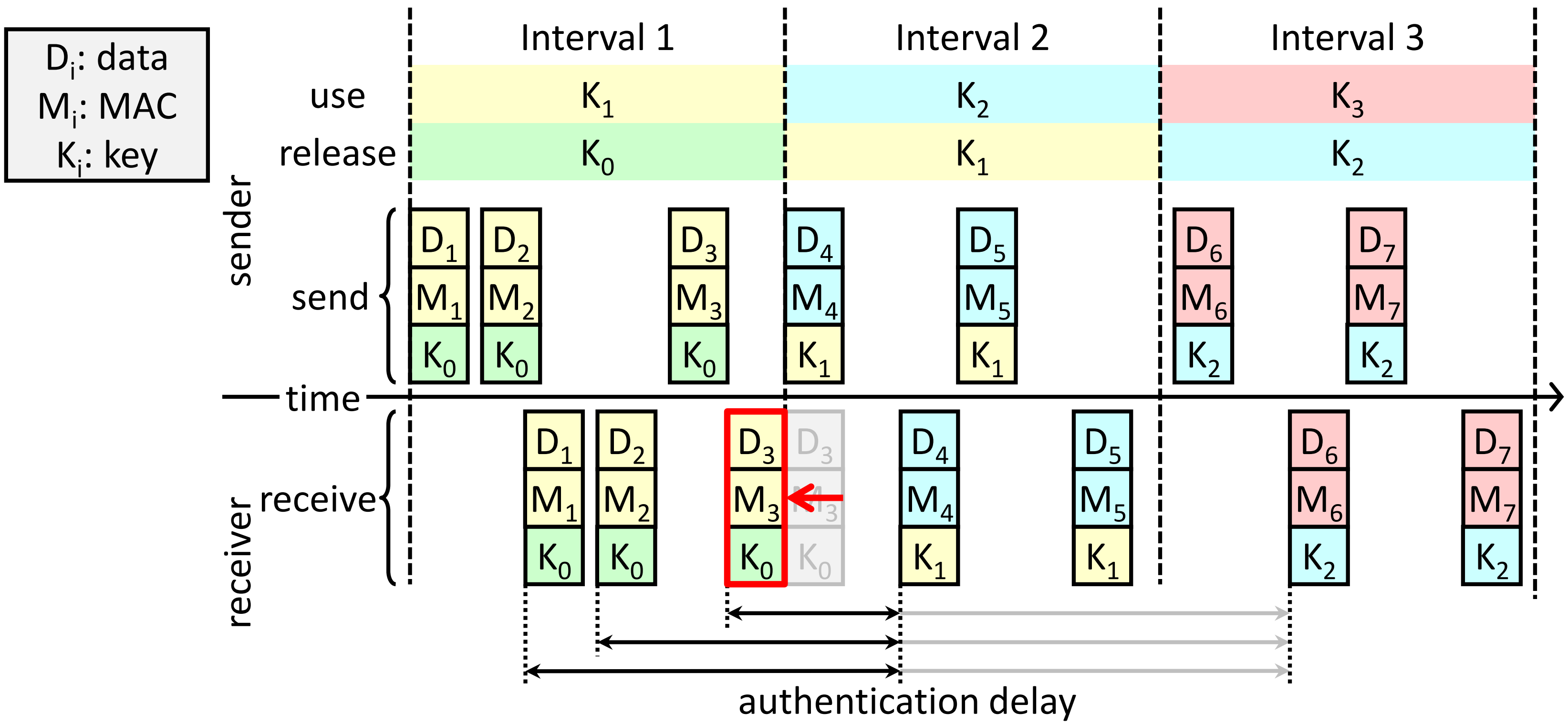
System Design (1/3)

- A scheduler schedules each sender's first instance within an interval earlier



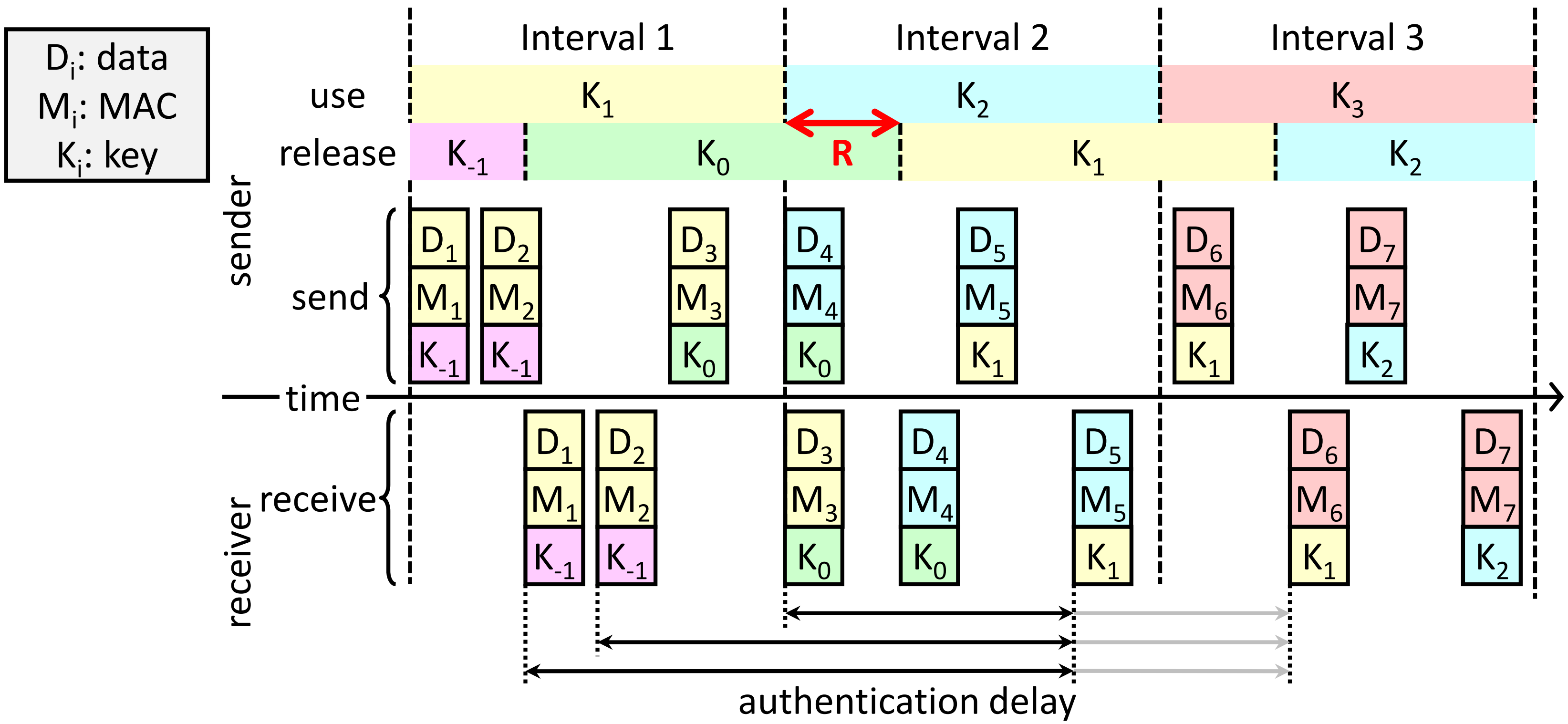
System Design (2/3)

- A scheduler schedules an instance earlier to ensure that it is received before the end of the interval
  - It can be regarded as a special case of the next approach



System Design (3/3)

- A scheduler minimizes the worst-case response time so that keys can be released earlier
  - R: the worst-case response time



Discussion

- How practical are the approaches?
  - One-key-for-all key distribution seems to be more practical

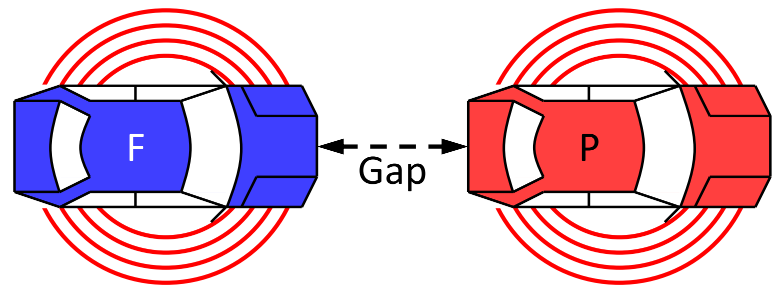
Outline

- ❑ Message Authentication
- ❑ **Jamming Analysis**
- ❑ Truthfulness Guarantee
- ❑ Intrusion Detection
- ❑ Consensus Algorithms
- ❑ Traffic Sign Design

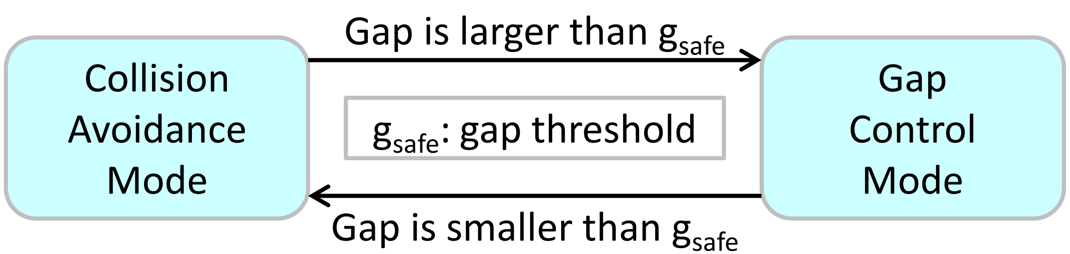
Cooperative Adaptive Cruise Control (CACC)

❑ Two CACC modes

- Gap control mode
  - The following vehicle (F) decides acceleration based on the gap, speeds, and accelerations of the two vehicles



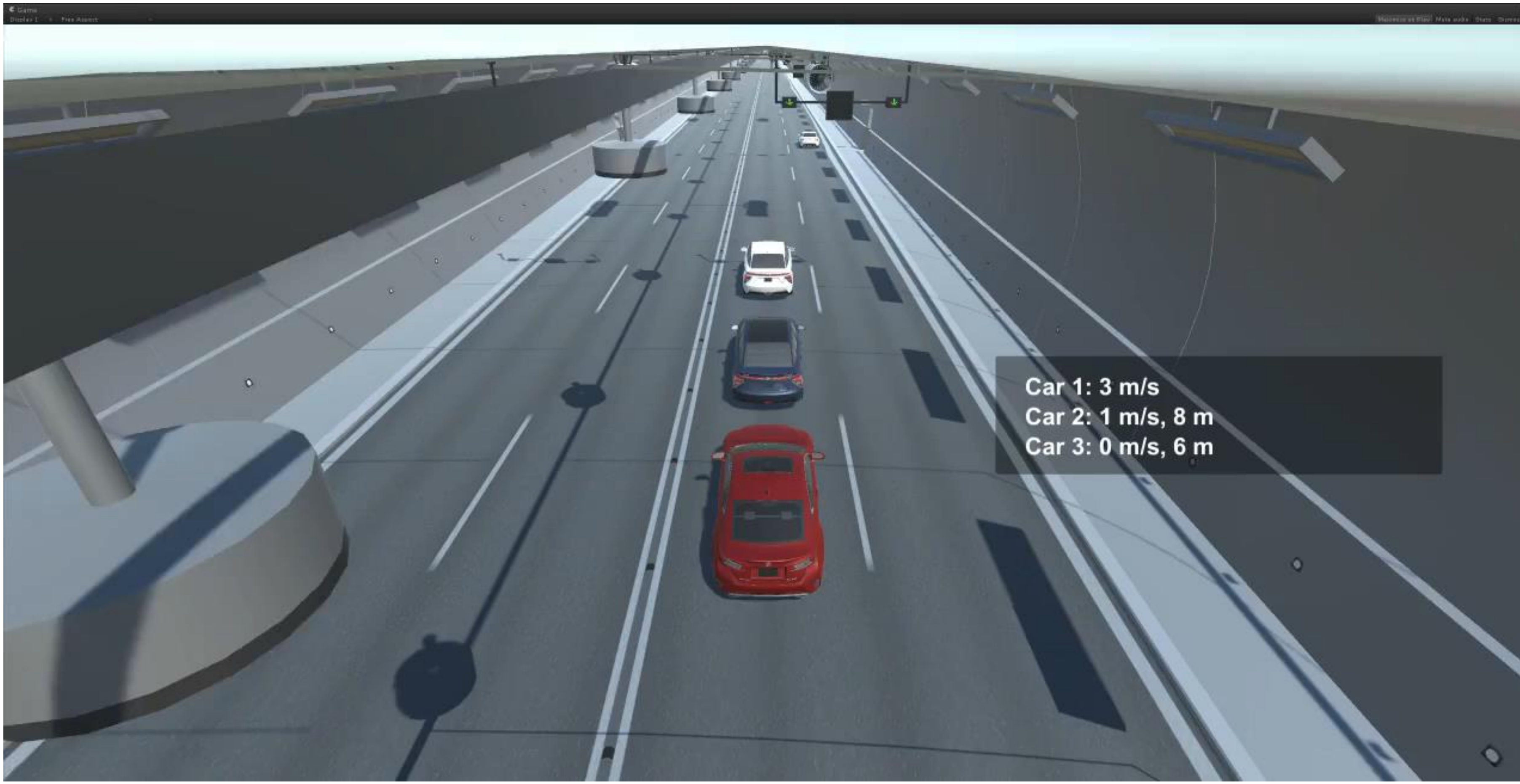
- Collision avoidance mode
  - The following vehicle (F) decelerates with its maximum deceleration



❑ Information sources

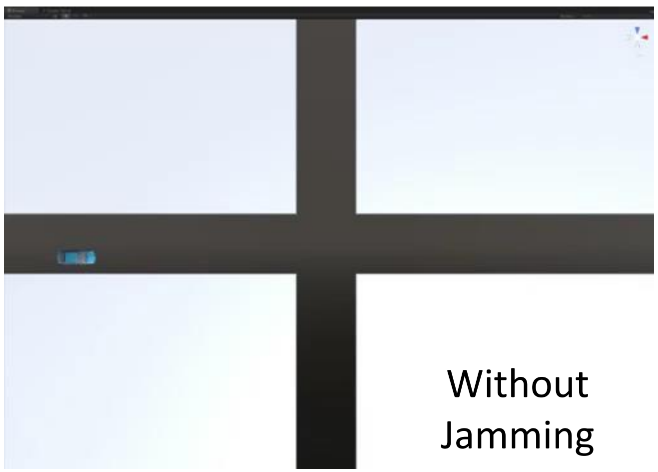
- Gap and speeds are obtained by sensors
- Accelerations are broadcasted with V2X messages

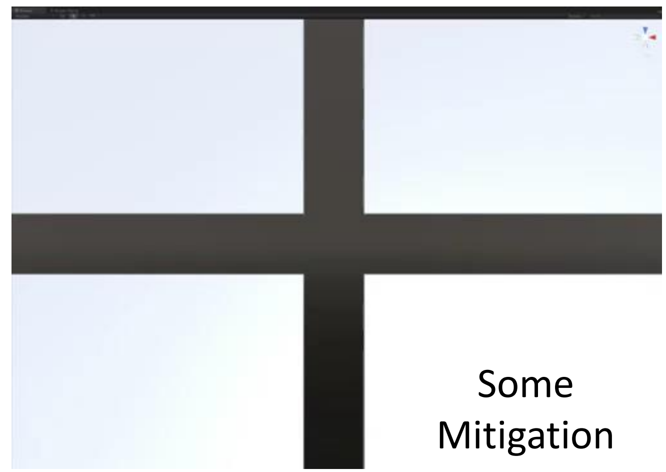
CACC under Attacks

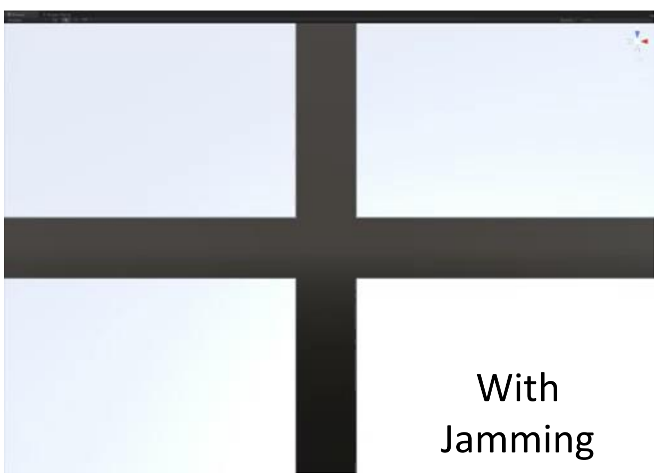


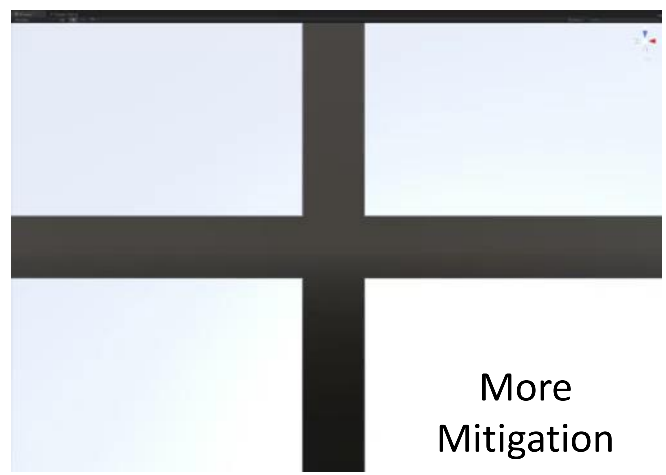
Intersection Management

- An intersection manager receives requests from vehicles, schedule them, and sends confirmations to them







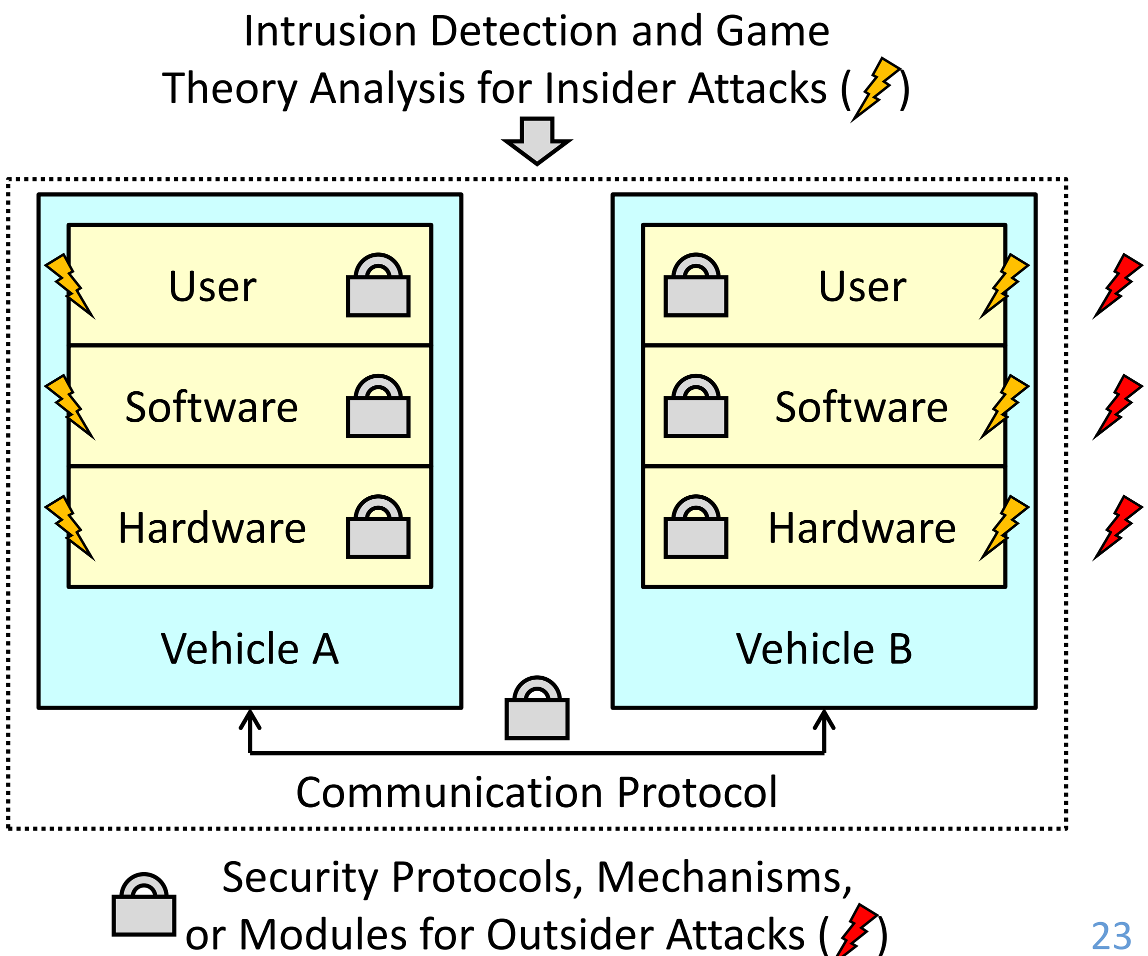


Outline

- Message Authentication
- Jamming Analysis
- **Truthfulness Guarantee**
- Intrusion Detection
- Consensus Algorithms
- Traffic Sign Design

Insider and Outsider

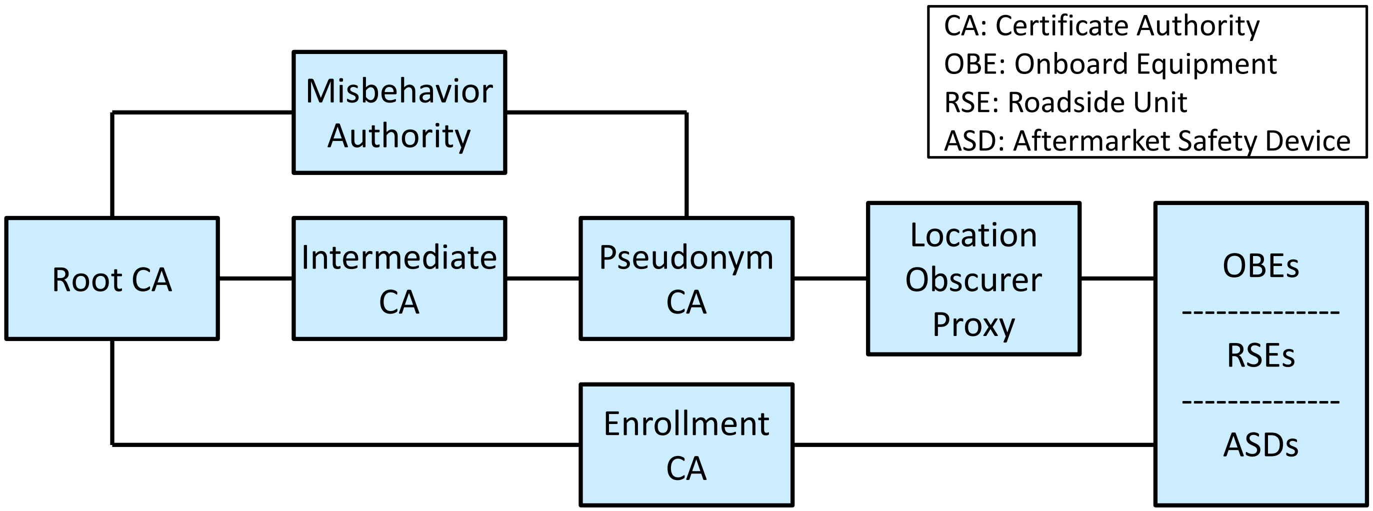
- Outsider: entity that cannot be authenticated
- Insider: entity that has been authenticated but compromised
  - Main focus
  - Examples
    - A sensor is tempered
    - A hardware or software implementation flaw is discovered
    - A secret key is leaked during manufacturing or design process
    - A legitimate user wants to take advantages
  - Note
    - Check DOT SCMS for outsider protection



Security Credential Management System

Protection against outsider attacks

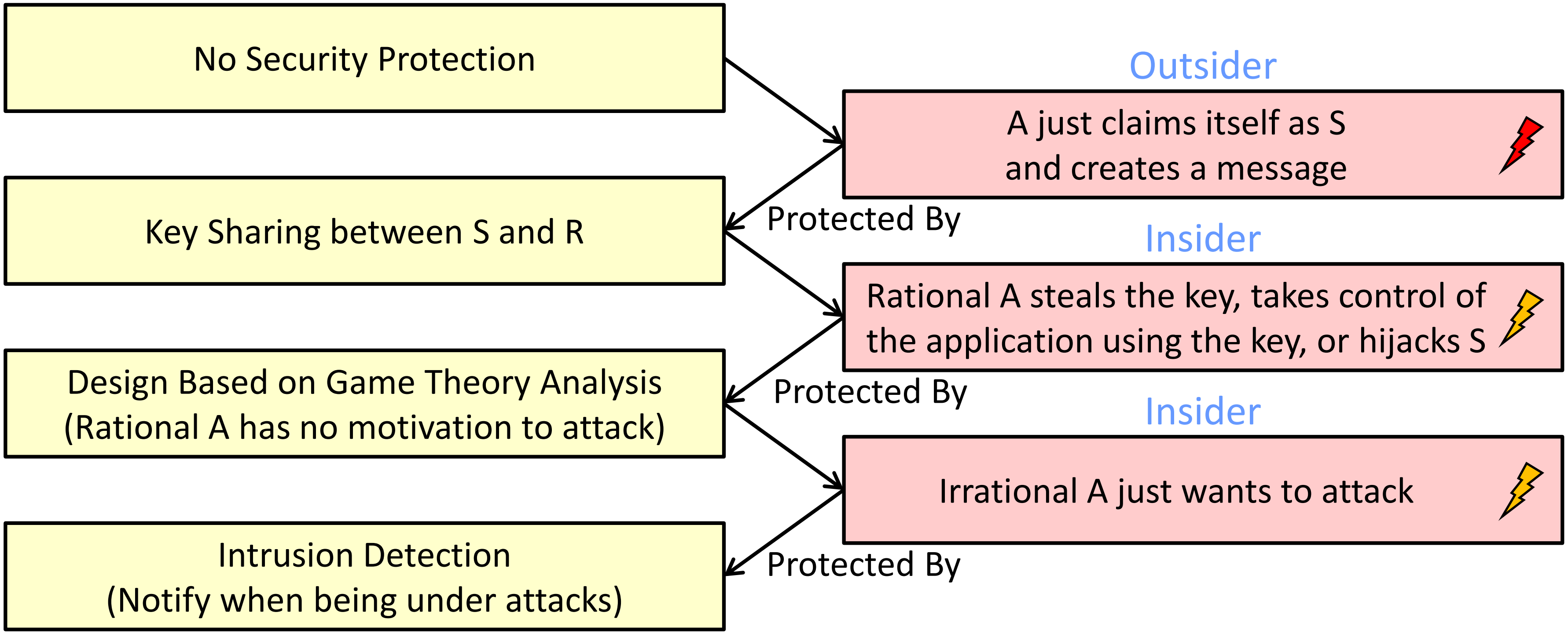
- A public key infrastructure (PKI) provides a means for distributing and verifying public keys in the form of digital certificates
- It works theoretically, but is there any limitation for connected cars in practice?



Roles of Different Security Protections

❑ Example

- S (sender) wants to send a message to R (receiver)
- A (attacker) wants to pretend as S, create a message, and get some advantages



Game Theory Analysis: Overview

- Using intersection management as an example
  - It can be generalized to other scenarios where multiple vehicles request and compete for some shared resource (e.g., an intersection) at some specific time
- Three-vehicle strategic game
  - Assume that the time needed to go through an intersection is 7

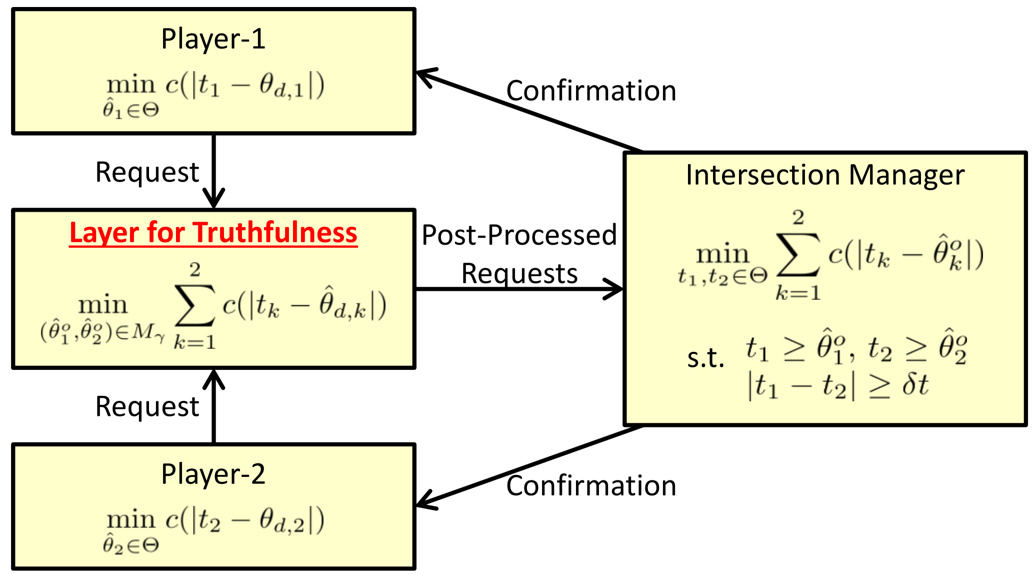
No Vehicle Lies				
Vehicle	Actual Time	Reported Time	Allocated Time	Delay
A	5	5	5	0
B	10	10	12	2
C	12	12	19	7
System Performance				9

Vehicle C Lies				
Vehicle	Actual Time	Reported Time	Allocated Time	Delay
A	5	5	5	0
B	10	10	19	9
C	12 ⟷	6	12	0
System Performance				9

  - Vehicle C does not worsen the overall system performance
  - However, vehicle C can take advantage from it

Game Theory Analysis: Approaches

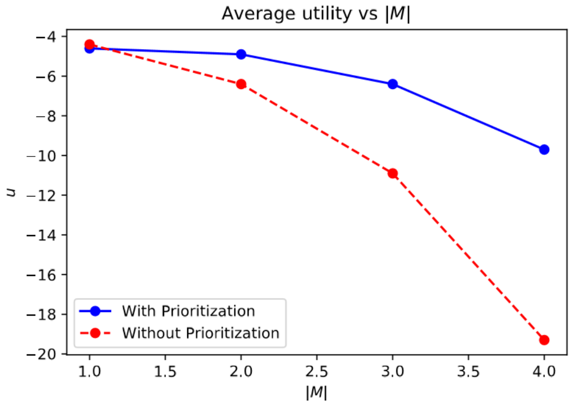
- Develop one additional layer for truthfulness
  - The layer leads the game to a Nash equilibrium
  - Rational players have no motivation to lie
  - The approach is limited to 2-vehicle scenarios so far

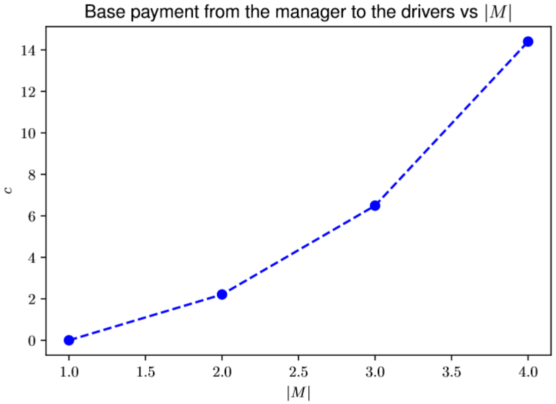


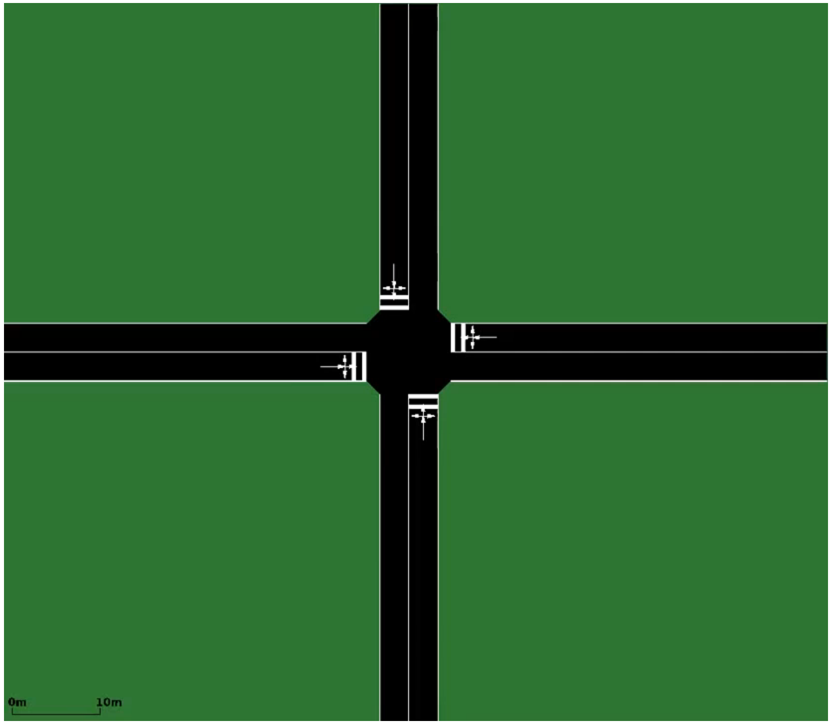
- Utilize payment to control
  - Rational players have no motivation to lie
  - The approach is not limited to 2-vehicle scenarios
  - Important application
    - This approach can also be used for users to report their "urgency" and pay (or get paid) to go through an intersection earlier (or later)

Game Theory Analysis: Results

- The payment-based approach supports prioritized intersection management where truthfulness is guaranteed
- An intersection becomes "more expensive" when there are more vehicles requesting the intersection







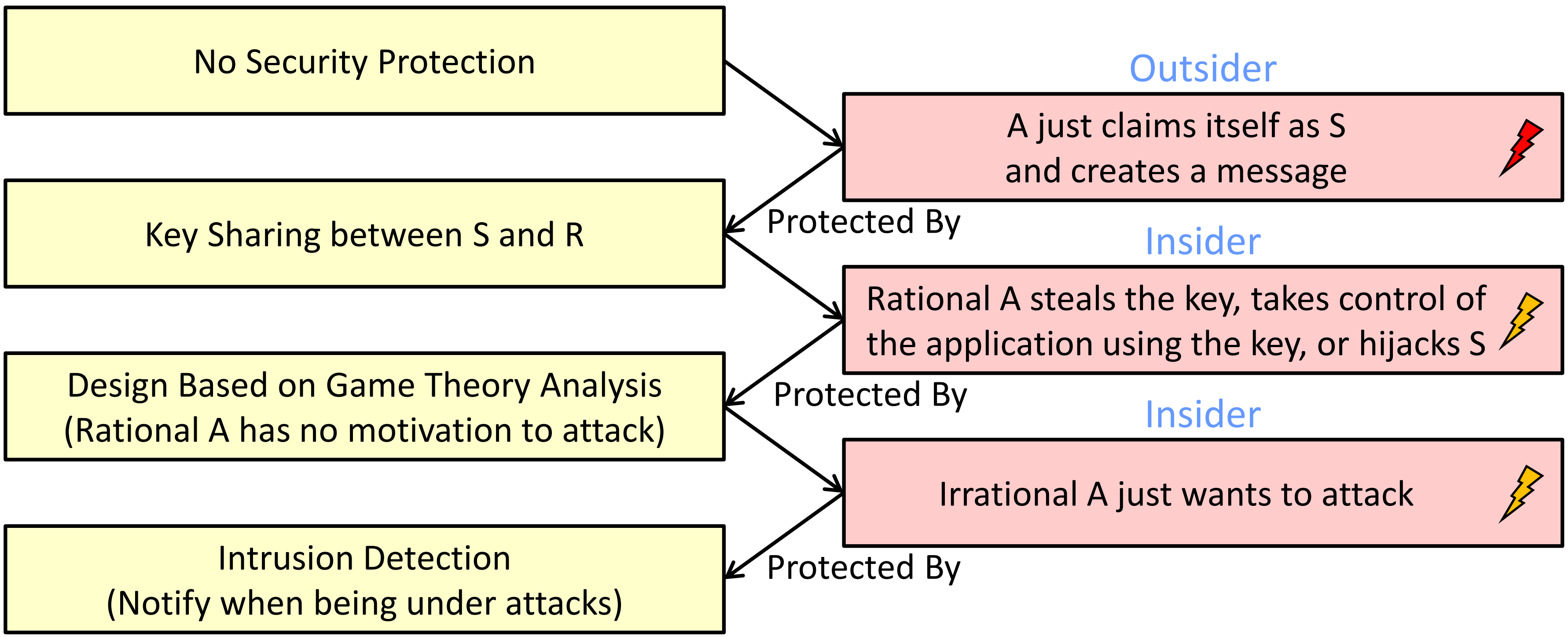
Outline

- ❑ Message Authentication
- ❑ Jamming Analysis
- ❑ Truthfulness Guarantee
- ❑ **Intrusion Detection**
- ❑ Consensus Algorithms
- ❑ Traffic Sign Design

Roles of Different Security Protections

❑ Example

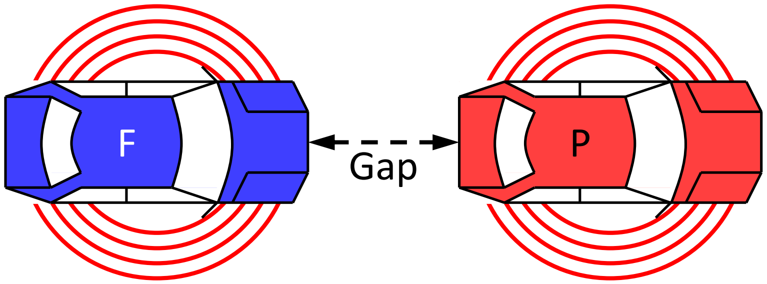
- S (sender) wants to send a message to R (receiver)
- A (attacker) wants to pretend as S, create a message, and get some advantages



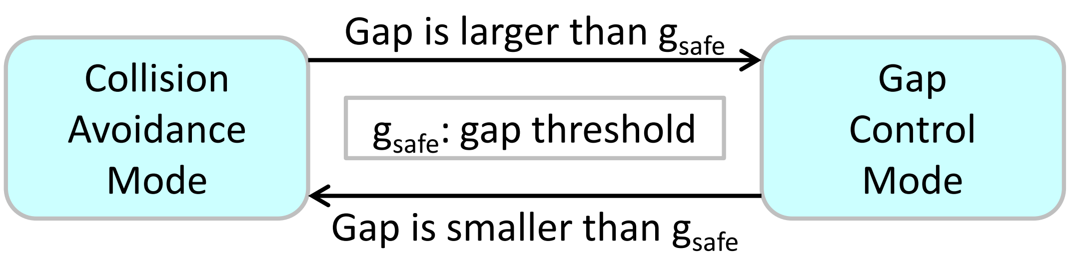
Cooperative Adaptive Cruise Control (CACC)

❑ Two CACC modes

- Gap control mode
  - The following vehicle (F) decides acceleration based on the gap, speeds, and accelerations of the two vehicles



- Collision avoidance mode
  - The following vehicle (F) decelerates with its maximum deceleration



❑ Information sources

- Gap and speeds are obtained by sensors
- Accelerations are broadcasted with V2X messages

Intrusion Detection: Overview

- Attacker models
  - A1 on acceleration: the leading car lies
  - A2 on velocity: velocity sensor lies about the leading car
  - A3 on position: position sensor lies about the leading car
  - A4 on velocity and position: A2 + A3
- Locations
  - In-car: limited computational resource, limited information
  - Edge: higher computational resource, more information
  - Cloud: highest computational resource, global knowledge, high latency
- Detection approaches
  - Physics-based detection (PHY)
  - Principal Component Analysis (PCA) based detection
  - Hidden Markov Model (HMM) based detection

Intrusion Detection: Attacks

	Stability	Efficiency	Safety
Metric	Jerk (m/s^3)	Waste (s)	Crash
No Attack	0.56	2.10	No
Attack A1 (on Acceleration)	7.07	3.14	No
Attack A2 (on Velocity)	0.60	9.31	No
Attack A3 (on Position)	0.73	N/A	Yes
Attack A4 (on Velocity + Position)	0.79	N/A	Yes

Intrusion Detection: Detectors

	PHY	PCA	HMM
Features	Simple and Quick (No Training Needed)	Catch Implicit Relationships	Catch Time-Series Data
In-Car	Applicable	Complexity Concern	Complexity Concern
Edge (Roadside Unit)	Applicable	Applicable	Applicable
Cloud	Latency Concern	Latency Concern	Latency Concern
Attack A1 (on Acceleration)	Detected	Detected	Detected
Attack A2 (on Velocity)	Not Detected	Detected	Detected
Attack A3 (on Position)	Not Detected	Not Detected	Detected
Attack A4 (on Velocity + Position)	Not Detected	Not Detected	Detected

Outline

- ❑ Message Authentication
- ❑ Jamming Analysis
- ❑ Truthfulness Guarantee
- ❑ Intrusion Detection
- ❑ **Consensus Algorithms**
- ❑ Traffic Sign Design

Consensus Algorithms

- Vehicles, road side units, edge servers, and cloud servers may have different opinions
  - Intrusion detection
  - Dynamic map creation
  - Event report checking
    - Examples: location, speed, and acceleration of a vehicle
- Challenges
  - If A says that B is wrong, is A or B actually wrong?
  - Timing-critical information
  - Vehicles are moving

Consensus Algo. in Distributed Systems

	Paxos	Laplacian	Blockchain	Gossip	Iterative	Weighted Average (Reputation System)
Need a Leader?	Yes	Yes	No	No	Yes	No
Robustness (against faulty or malicious nodes)	Very High	High	Very High	Average	High (as Iterations Go)	Low
Computational Overhead	High	Depends on Topology (Higher Connectivity, Lower Overhead)	Depends on "Puzzles"	Low	Depends on Topology and # of Iterations	Low in Most Cases
Communication Overhead	High	Depends on Topology	Depends on Detailed Design	Average/Low	High	Low in Most Cases
Scalability	Average	Average	Low in Basic Design	High	N/A	High
Reliability (e.g., against unstable communication)	Very High	High	Very High	Low	High	Low

Outline

- ❑ Message Authentication
- ❑ Jamming Analysis
- ❑ Truthfulness Guarantee
- ❑ Intrusion Detection
- ❑ Consensus Algorithms
- ❑ **Traffic Sign Design**

Traffic Sign Design as a Game

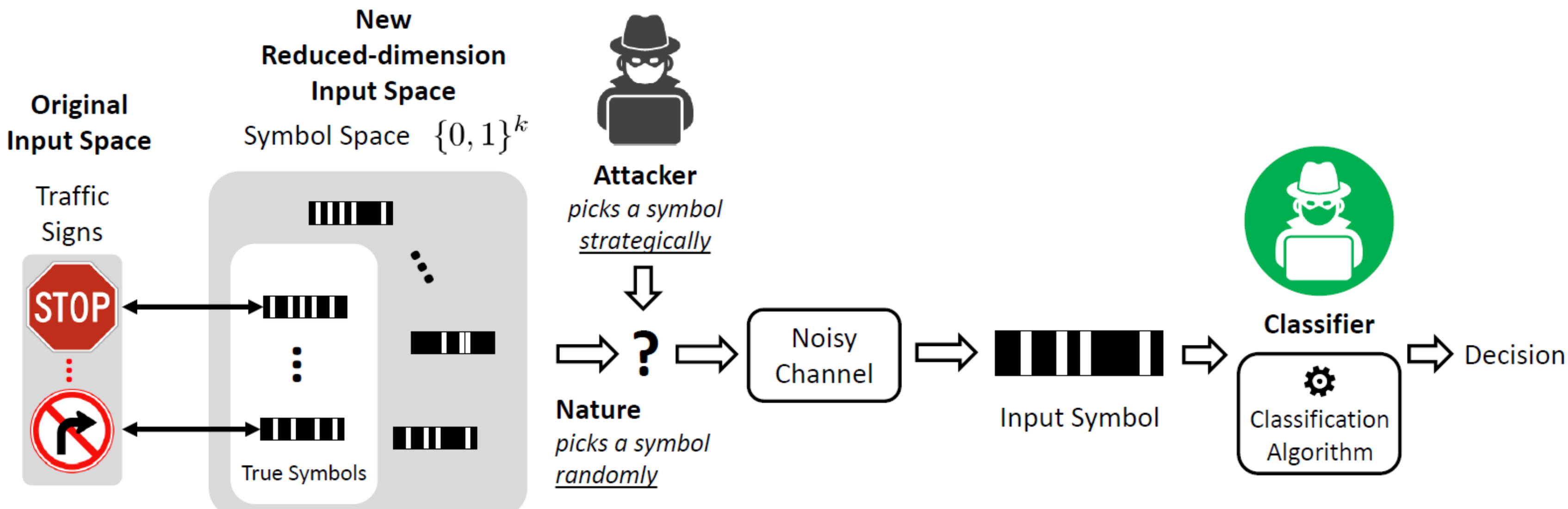
- Adversary classification

Machine Learning Classifier

There is no stop sign!

[CVPR '18]

- How if we add barcodes to traffic signs?



Q&A