Corso Professionalizzante di Specializzazione (3 CFU)

Ingegneria dell'Informazione o magistrale in Ingegneria Informatica
Automatica, Ingegneria Elettronica,
Ingegneria delle Telecomunicazioni

WSN and VANET Security

Part I: Generalities on WSN and VANET Security

Lecture I.4

Cyber Attackers and Attacks

Ing. Marco Pugliese, Ph.D., SMIEEE
Senior Security Manager cert. UNI 10459-2017
marpug@univaq.it

April 19th, 2024

Outline

- Classification of Cyber attackers
- Classification of attacks
- Cyber attacks against WSN
- Cyber attacks against VANET
- Cyber attacks against Intra-Vehicle Communications
- Classification of the Security Functions

Classification of Cyber attackers

- **Outsiders vs. Insiders**
  - insiders are authenticated into network
  - outsiders not
- **Malicious vs. Rational**
  - malicious attackers cause accidents just for fun
  - **rational** attackers do so for specific purposes
- **Active vs. Passive**
  - active attackers send fake or modified messages to other nodes
  - passive attackers only monitor the network and eavesdrop on communications between other nodes to collect useful information for future attacks
- **Local vs. Extended**
  - local attackers only perpetrate attacks in a limited range
  - extended attackers attack across the network
- **Mote class vs. Laptop class**
  - mote class attackers have enough resource to attack few low-energy nodes (motes) with similar capabilities
  - laptop class attackers have enough resource to attack many motes or few high-energy nodes with similar capabilities

Outline

- Classification of Cyber attackers
- Classification of attacks
- Cyber attacks against WSN
- Cyber attacks against VANET
- Cyber attacks against Intra-Vehicle Communications
- Classification of the Security Functions

Classification of attacks

- **Network Attack (NA):** objective is damaging the **communication reliability at network level** by limiting or deleting the availability of the network and the services it offers: DOS (Denial of Service) and DDOS (Distributed DOS) attack falls into this class.

- **Timing / Sync Attack (TA):** objective is damaging the **communications reliability at local link level** by changing time slots and / or by altering synchronization mechanisms to generate a delay in the transmission of packets. Strong impact on "time critical applications“.

- **Application Attack (AA):** objective is damaging the **service reliability** by changing the content of service messages generated. Serious impact in VANET.

- **Monitoring Attack (MA)**: objective is damaging the **service confidentiality** by spying nodes (vehicles) communications through the compromission of existing monitoring systems.

Reference attacks

- **Denial Of Service (DOS)**: inferring malfunctions to single parts or to the whole network. The main objective is to ensure that authorized users do not have the opportunity to access the services or resources offered by the network. It represents an attack on network availability and access control functions.

  A more aggressive modality is the coordinated and distributed DOS (DDOS): in this case, the attackers (daemons) launch attacks from different points of the network to cover a large area of the network itself.
- **Spoofing**: altering data, e.g. from sensors. Sensing data return the environmental context to application services and therefore even slight alterations on these data can lead to serious consequences to service users (e.g. in VANET the GPS signal). It represents an attack on authentication, confidentiality and traceability functions.
- **Eavesdropping**: intercepting communications to take useful information contained in the messages to be used later for specific purposes. It represents an attack on authentication, confidentiality and traceability functions.

Reference attacks

- **Identity hijacking**: pretending to be someone else using a different ID. It represents an attack on authentication, confidentiality, non-repudiation, traceability and access control functions
  - **Sybil**: the attacker sends a series of messages with different IDs with a certain frequency to the other nodes to make believe that they have been generated by different nodes (vehicles) and simulate traffic on the road network. The goal is to convince other nodes / vehicles to change their route so that the attacker can reap personal benefits. The Sybil attack therefore damages the network topology and causes excessive consumption of the available bandwidth.
  - **Session hijacking**: the attacker takes the Session Identifier (SID) assigned to each session and through this takes control of the session already established.
  - **Replay attack**: the attacker pretends to be an authorized user through the use of previously received or captured messages which are then repeated in different parts of the network infringing the authenticity and confidentiality of the system.

Outline

- Classification of Cyber attackers
- Classification of attacks
- Cyber attacks against WSN
- Cyber attacks against VANET
- Cyber attacks against Intra-Vehicle Communications
- Classification of the Security Functions

Physical Layer Vulnerabilities

- Exposure to adverse weather conditions
- Unattended deployment
- Wireless communications
- HW packaging

Attacks against Physical Layer

Side Channel Attack (Network Attack, DOS)

- This attack is based on power consumption information gathered from the physical implementation of a cryptographic hardware device then analyzes the collected data to extract the associated crypto key.
- The attack can non-invasively extract cryptographic keys and other secret information from the device.
  - **Simple power analysis** (**SPA**) involves visually interpreting power *traces*, of electrical activity over time (variable currents induce EM fields).
  - **Differential power analysis** (**DPA**) a more advanced form of power analysis, used to extract secret keys and compromise the security of tamper resistant devices. DPA is a side-channel attack that is extremely effective low cost and widely known. These attacks use variations in the electrical power consumption of a targeted device and then breech security in devices by using statistical methods by deriving secret keys from crypto-algorithm. DPA attacks are noninvasive, an intruder can compromise an embedded system **without leaving a trace**.

Attacks against Physical Layer

Jamming Attack (Network Attack, DOS, Spoofing)

- The adversary attempts to disrupt the operation of the network by broadcasting a high-energy signal.
  - **Constant jamming**: corrupts packets as they are transmitted.
  - **Deceptive jamming**: sends a constant stream of bytes into the network to make it look like legitimate traffic
  - **Random jamming**: randomly alternates between sleep and jamming to save energy.
  - **Reactive jamming**: transmits a jam signal when it senses traffic.

- Spread spectrum techniques in radio communications are used to protect against this attack.

Attacks against Physical Layer

Node Capture Attack (Network Attack, DOS)

- The attacker gains full control over a sensor node through a direct physical access. In such case, the attacker can extract cryptographic primitives (key material, e.g. private key) and obtain unlimited access to the information stored on the memory chip of the captured node through a reverse engineering process
- Some factors can aid the attackers during a node capture attack:
  - If these nodes **share a key** ("shared secret") with neighbour nodes used to encrypt or decrypt data.
  - If these nodes have a great impact on the structure or topology of a WSN.
- The cryptographic key **should not be preloaded**
  - Avoid preloading shared master keys or session keys
  - Allow cryptographic keys to depend on more than one single node (authentication by topology and not only by identity).

Attacks against Physical Layer

Tampering Attack (Network Attack, DOS, Spoofing)

- **The simplest way to attack is to damage or modify sensors physically and thus stop or alter their services**. The impact will be greater if base stations or aggregation points are attacked, since these nodes have a major critical role in data communications and/or data processing.
- A defense to this attack involves **tamper-proofing** the node's physical package and security information self destruction – whenever somebody accesses the sensor nodes physically the node **erases its memory and prevents any leakage of information**.

Data Link Layer Vulnerabilities

- Protocol synchronizations
- Exchange of uncyphered messages (e.g. PANid, GTS management)
- Algorithm complexity (CSMA, collision avoidance, nonce)
- Superframe time slotting

Attacks against Data Link Layer

Back-off Manipulation Attack (Timing Attack, DOS)

- In IEEE 802.15.4 and, more in general, in network using CSMA mechanisms to access the same physical medium simultaneously, the data being transmitted could be corrupted.
- In CSMA the sender listens to the channel before transmitting its packet: if the channel is found busy the sender will defer its access by an amount of time which is called **back-off period**. CSMA gives the recent channel access to the contending node with the smallest back-off value.
- An attacker can manipulate the back-off value: illegitimately **by assigning a large back-off interval to prevent medium access or, vice-versa, by assigning small back-off interval to favor it**.

Attacks against Data Link Layer

Attacks to ACK (Timing Attack, Identity hijacking)

- In the middle of a transmission between two legitimate users, an eavesdropper **can listen to the unencrypted sequence numbers of the frames**. When the eavesdropper wants to prevent the legitimate receiver from getting a frame, it corrupts the frame by interfering at the receive time. Then, the eavesdropper sends a fake ACK frame with the related sequence number to the sender in order to fool the sender as if the ACK was coming from the receiver.
- This attack can also be applied to RTS/CTS handshake in CSMA/CA.

Attacks against Data Link Layer

PANId Conflict Attack (Timing Attack, Identity hijacking, DOS)

- In 802.15.4, a PAN (Personal Area Network) includes one PAN Coordinator and a group of PAN members.
- PAN members know the PAN Coordinator's Identifier (PANId). If there exists **more than one PAN Coordinator operating in same domain**, a PANId conflict could occur: in this case, the PAN Coordinator may detect the conflict through its received beacons or one of the PAN members can notify the PAN Coordinator on receiving signal from two PAN coordinators with same PANId.
- Therefore the PAN Coordinator performs the conflict resolution procedure: this mechanism mainly covers the channel scans and coordinator realignment procedure that includes choosing a new PANId and broadcasting it to all PAN members.
- **This procedure is energy and time consuming and induces a permanent unavailability of a valid PANId which degrades data transmissions**.

Attacks against Data Link Layer

GTS Attack (Timing Attack, Identity hijacking, DOS)

- According to IEEE 802.15.4 standard, **GTS is the portion of the superframe reserved for a specific device which provides contention free communication** between the device and the coordinator in beacon enabled mode.
- The GTS attack can be described as follows:
  - The attacker **has achieved synchronization with the PAN Coordinator by receiving beacon messages**.
  - The attacker can learn the GTS times of the coordinator through extracting the GTS descriptor within beacon frame: **the GTS descriptor indicates the length and the start of the GTS in the superframe**.
  - After obtaining the allocated GTS times, **the attacker can create interference / collisions / data packet corruption at any moments**.

Attacks against Data Link Layer

Continuous Channel Access (Exhaustion) Attack (Network Attack, DOS)

- A malicious node disrupts MAC protocol **by continuously requesting or transmitting over the channel**
- This eventually **leads a starvation for other nodes** in the network with respect to channel access
  - **Apply Rate Limiting to the MAC admission control** such that the network *can ignore excessive requests*, thus preventing the energy drain caused by repeated transmissions.

Attacks against Data Link Layer

Interrogation Attack (Timing Attack, DOS)

- Exploits the two-way RTS/CTS handshake: an attacker can exhaust a node's resources by repeatedly sending RTS messages to induce CTS responses from a targeted neighbor node.

Collision Attack (Timing Attack, DOS)

- A collision occurs when two nodes attempt to access simultaneously over the same medium: electrical interference can cause alterations in payload content causing **a checksum mismatch at the receiving end. The packet will then be discarded as invalid**.

DoS Attack (Timing Attack, DOS)

- An attacker repeatedly **jams the medium during both the Contention Access Period (CAP) and the Contention Free Period (CFP)**. In this way, a victim device can be put on endless retransmission loop, which ultimately leads to a battery exhaustion of a victim device or at least greatly reduces its battery life.

Network Layer Vulnerabilities

- Network topology unstability
- State alignment (routing tables) for proactive routing protocols
- Update delays for reactive routing protocols
- Exchange of unciphered / unauthenticated messages

Attacks against Network Layer

Routing Attack (Timing Attack, DOS, Spoofing, Identity hijacking)

- Any WSN node acts as a router
- Routing vulnerabilities include integrity of tables entries and state transitions in proactive protocols and integrity of setup message flooding in reactive protocols.
- This attack aims to create **fake links from legitimate nodes to unlegitimate nodes and viceversa**
- Some of the attacks are the following:
  - Wormholes attack
  - Selective forwarding attack
  - Sinkhole attack
  - HELLO flood attack

Attacks against Network Layer

Injection Attack (Timing Attack, DOS, Spoofing)

- Transmit malicious routing information into the network resulting in routing inconsistencies **(state-less routing protocols)**

Traffic Misdirection Attack (Timing Attack, Spoofing, DOS)

- Diverting traffic away from intended destination **(state-based routing protocols)**

Attacks against Network Layer

Traffic Analysis Attack (Monitoring Attack, Eavesdropping, Spoofing)

- An attacker is able to gather much information on the topology of the network as well as the location of the base station and other strategic nodes **by observing traffic volumes and patterns**.
- There are two types of traffic analysis attacks in WSNs: a rate monitoring attack and a time correlation attack.
  - In a **rate monitoring attack** an attacker monitors the packet sending rate of nodes near the attacker and **moves closer to the nodes that have a higher packet sending rate**.
  - In a **time correlation attack** an attacker observes **the correlation in sending time between a node and its neighbour node that is assumed to be forwarding the same packet** and deduces the path by following the sound for each forwarding operation as the packet propagates towards the base station.

Transport Layer Vulnerabilities

- Time synchonization
- Exchange of unciphered / unauthenticated messages

Attacks against Transport Layer

Attacks on Time Synchronization (Timing Attack, DOS)

- Time synchronization protocols provide a mechanism **for synchronizing the local clocks of nodes in a sensor network**.
- An attacker can physically capture a fraction of the nodes and injecting them with faulty time synchronization message.
- This event can make the nodes in the entire network out-of-sync with each other.

Vulnerability Resume

- Distributed Computing
- Exchange of unciphered / unauthenticated messages

Attacks against Application Layer

Software Code Attack (Application Attack, DOS)

- An attacker may try to **modify the software code** in memory or exploit known vulnerabilities in the software code.
- A well-known example of such an attack is a buffer overflow attack where a process attempts to store data beyond the boundaries of a fixed length buffer, thus, resulting in the extra data overwriting the adjacent memory locations.

Attacks against Application Layer

Attack to Cluster Management (Application Attack, DOS)

- Protocols for cluster management are required to do:
  - Supervision of new cluster head identification
  - Admission of new group members
  - Management of the group consistency (i.e. verification of the existence of a unique cluster head, manage the fault of the cluster head, …)
- Attacks are based on the alteration of information related to these functions

Attacks against ZigBee

- Zigbee PRO 2023 (the current version) expands on secure-by-design architecture by adding a number of security enhancements: the **Dynamic Link Key, the Device Interview and Trust Center Swap Out**.
  - Dynamic Link Key is a significant improvement based on Public/Private key pairing and advanced security curves, further protecting the network from attacks.
  - Device Interview technology allows users to query and filter out the devices before allowing them onto a network based on ecosystem requirements.
  - The Trust Center Swap-Out feature allows changing out the “Trust Center” which can be a gateway, hub, smart speaker, and even commercial electric meters for a network without requiring all devices to be recommissioned.
- In addition to the security improvements, Zigbee devices built to Zigbee PRO 2023 specifications with a sufficient level of security are now able to be on the same network as Smart Energy devices, providing the exchange of important information to further improve control and use of the energy and devices.

Outline

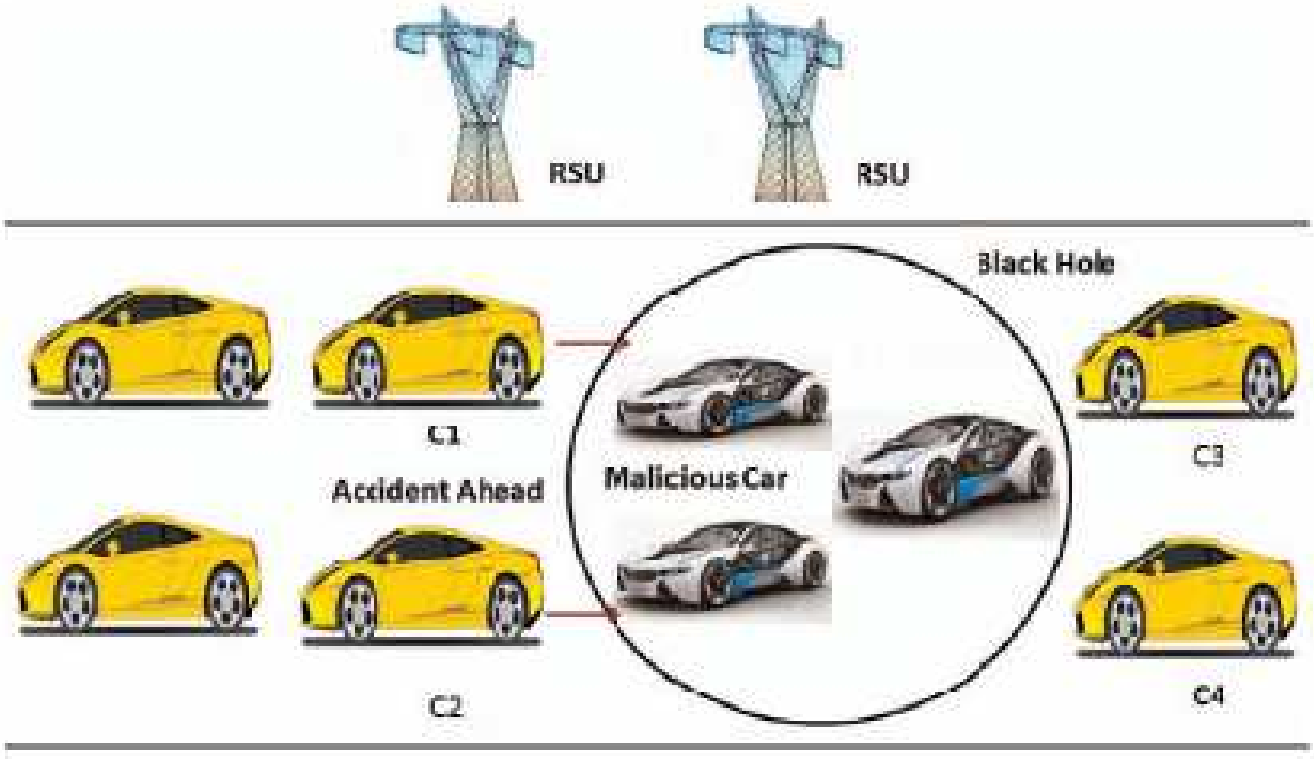
- Classification of Cyber attackers
- Classification of attacks
- Cyber attacks against WSN
- Cyber attacks against VANET
- Cyber attacks against Intra-Vehicle Communications
- Classification of the Security Functions

Vulnerability Resume

- The same as WSN
- Privacy issues
- DOS attacks can be based only on delay
- Exchange of unciphered / unauthenticated messages

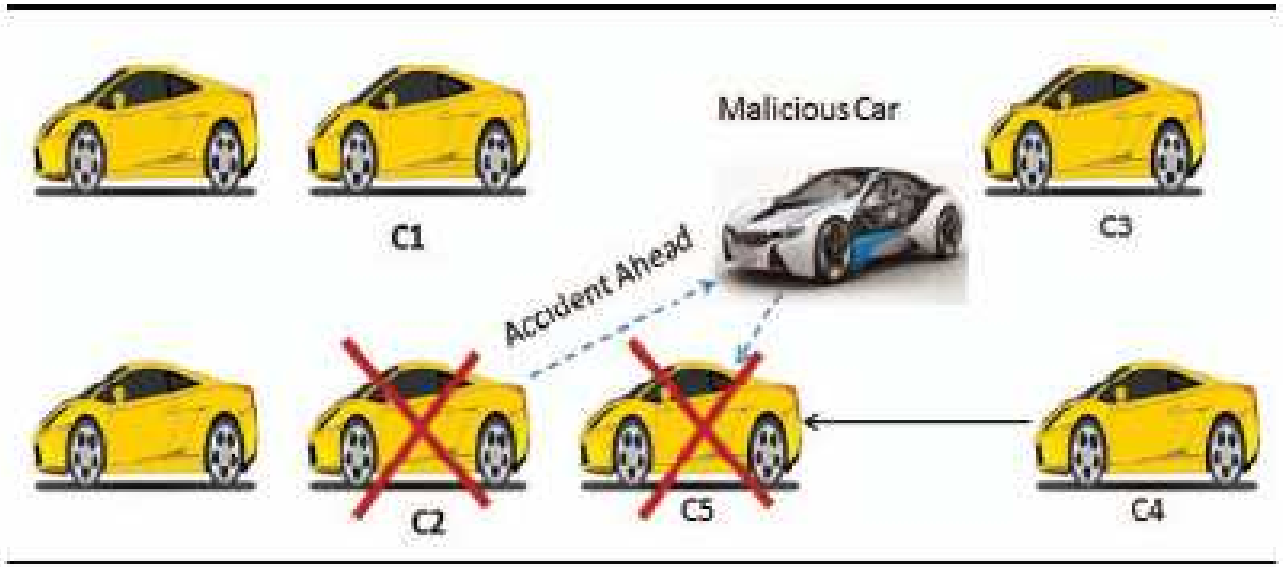
Sinkhole

- Figure shows C1 and C2 transmitting data packets destined to C3 and C4, respectively. **But the packets at first reach the black hole with many malicious cars**. Data packets are lost in black hole, resulting in C3 and C4 never receiving the packet.



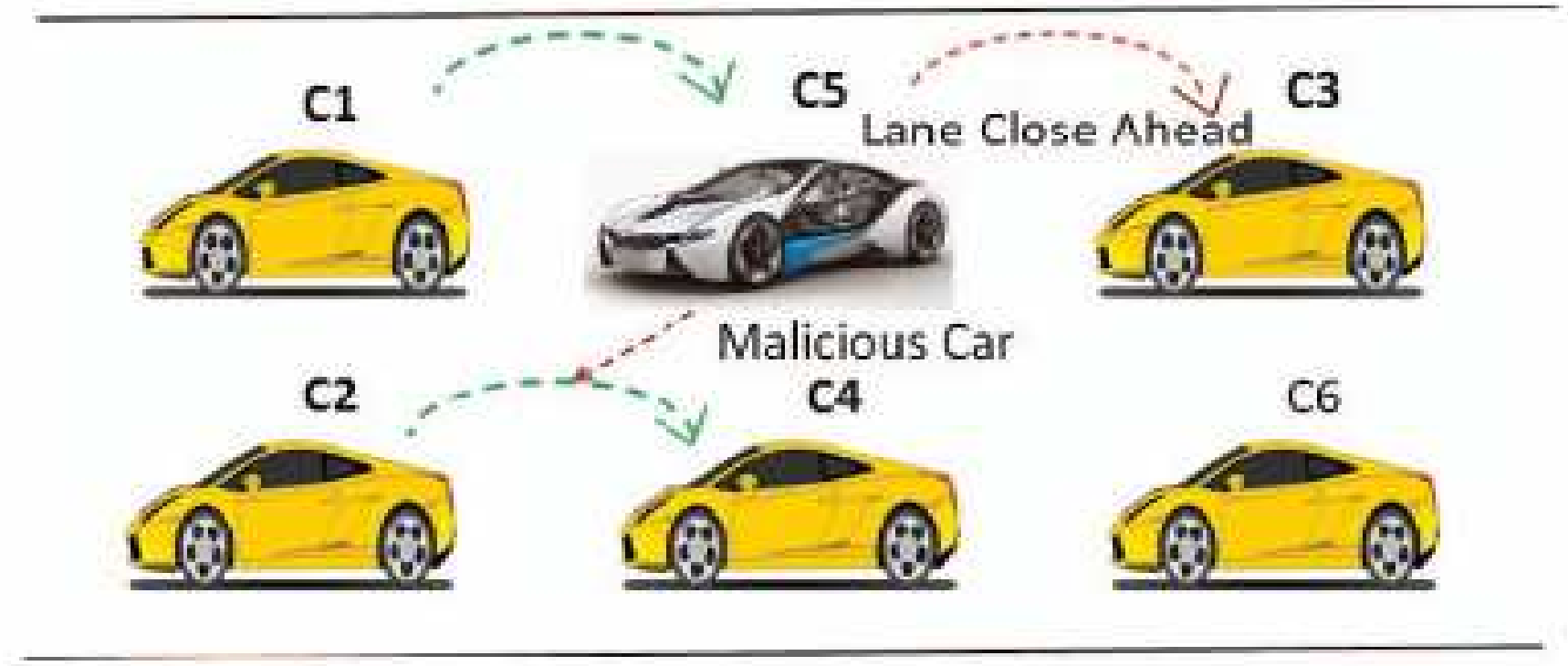
Timing Attack

- Figure shows a malicious car receives a message “accident ahead” from C2 but **it doesn’t transmit the message immediately but adds some timeslots to the message, so this message is received by a car in position C5 (accidental position) instead of a safe position C4**.
  - An attacker selectively drops packets of messages from the network, which may hold critical information for the intended receiver, and the attacker suppresses these packets and can use them again in the future.
  - A goal of such an attack would be to prevent registration and insurance authorities from learning about collisions involving the attacker’s vehicle and/or to avoid delivering collision reports to roadside access points.



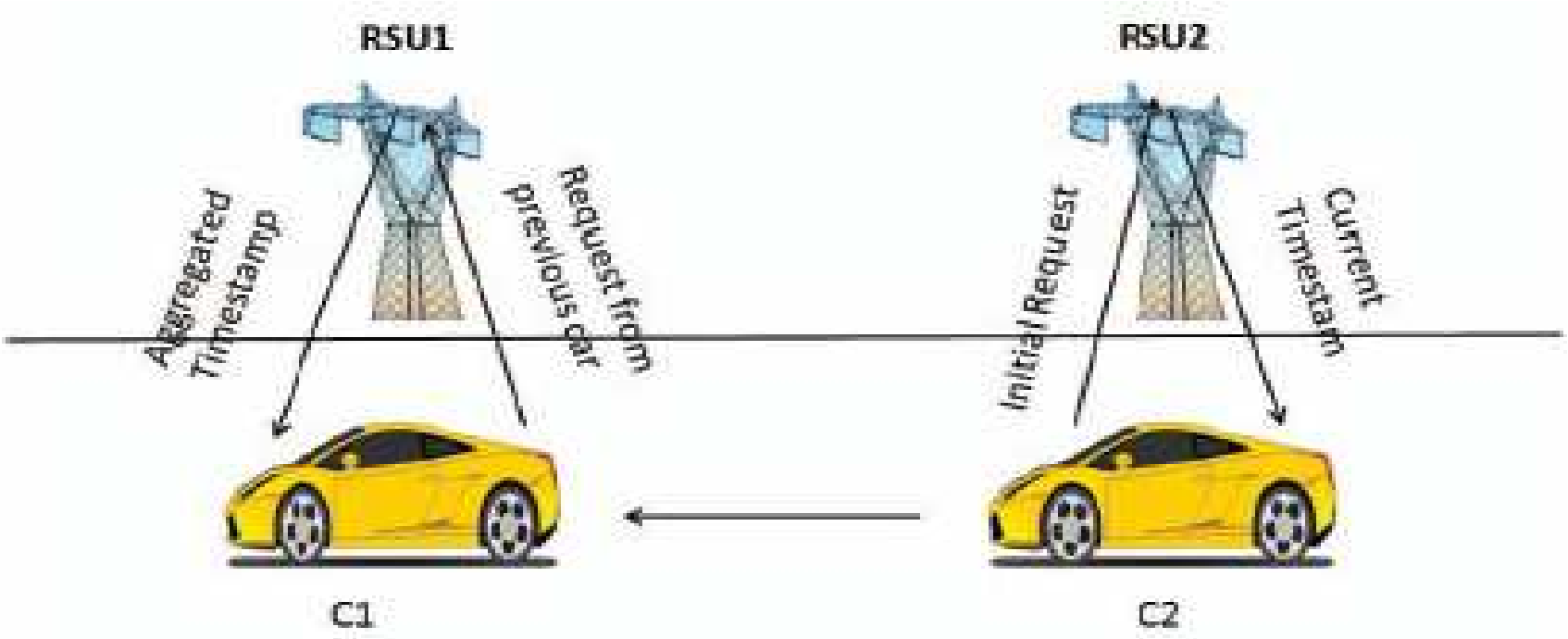
Man In the Middle (MIM)

- Figure shows a malicious car C5 listens to the communication between C2 and C4 and **transmits wrong information** to C3 which C5 receives from C1.
  - A malicious car can overhear communication between two vehicles. To launch an attack, a malicious car inserts the wrong information between communicating vehicles.



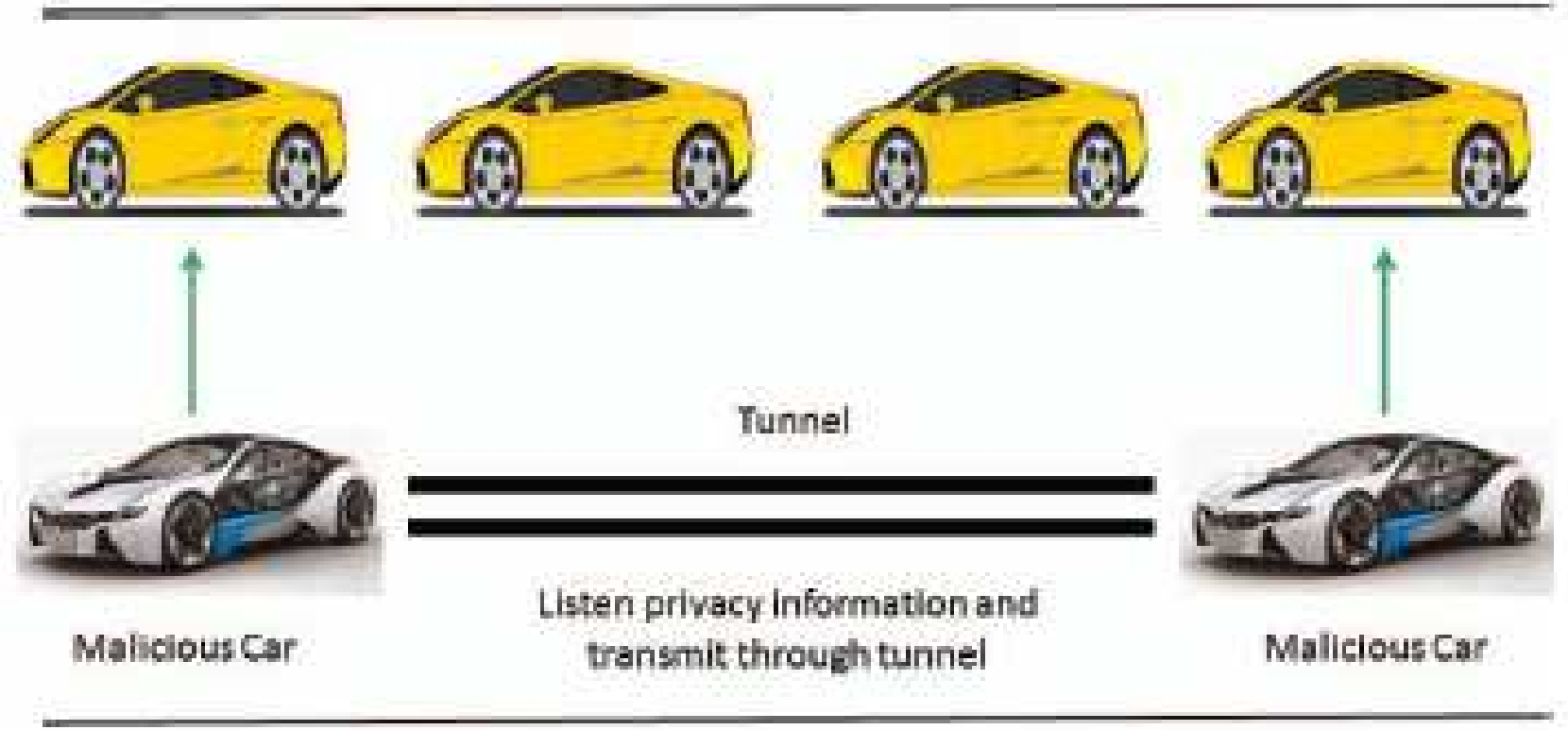
Sybil

- It is assumed that only one vehicle can pass an RSU at a timestamp. RSU issues a digital certificate for the vehicle that passes through.
- Figure shows the **malicious Sybil car that gets several messages with common timestamp certificate**.
  - A single malicious node may produce different identities thereby, transmits messaging that seem to be from different legitimate vehicles. Other legitimate vehicles think the network has many vehicles which is not the case.

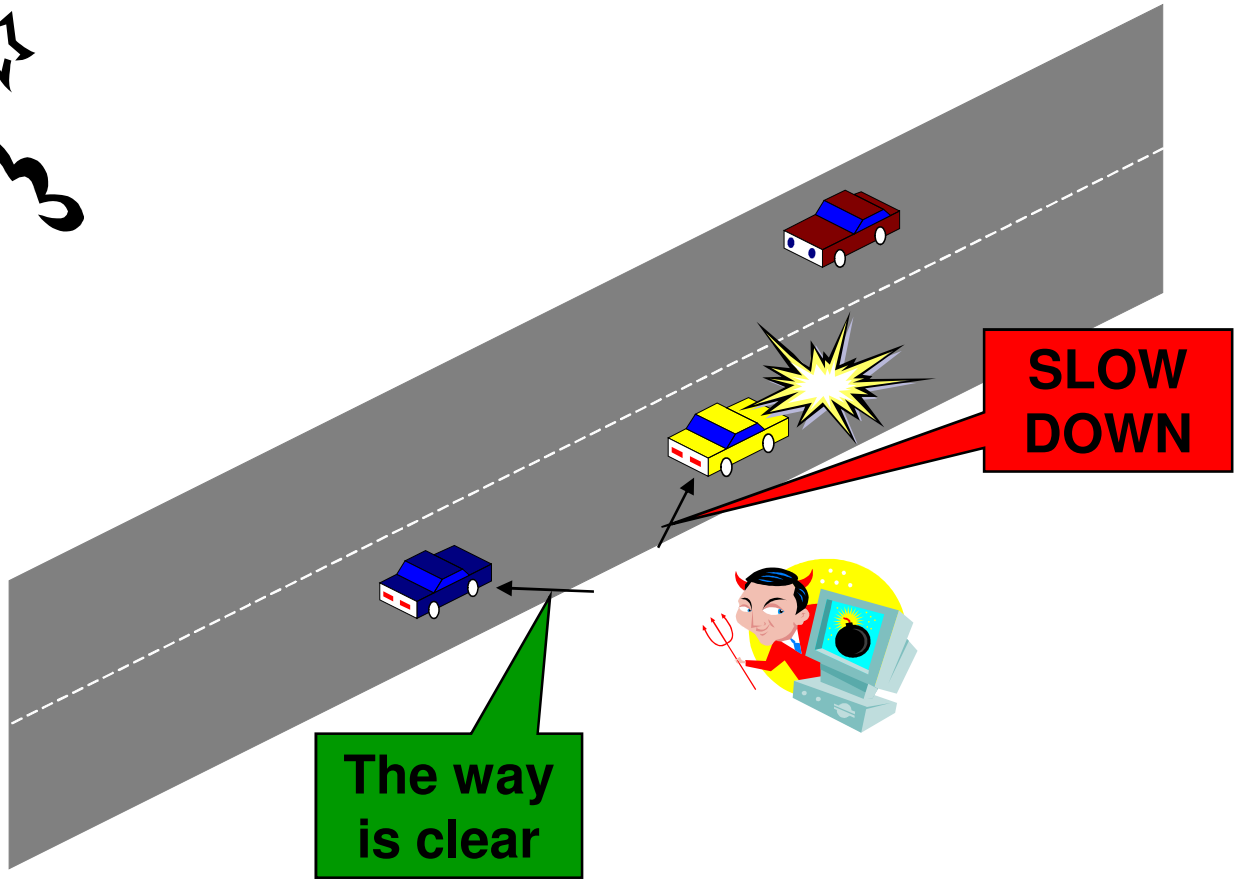


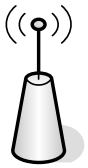
Wormhole

- Figure shows two attackers at two sides **creating a tunnel to broadcast malicious information**.

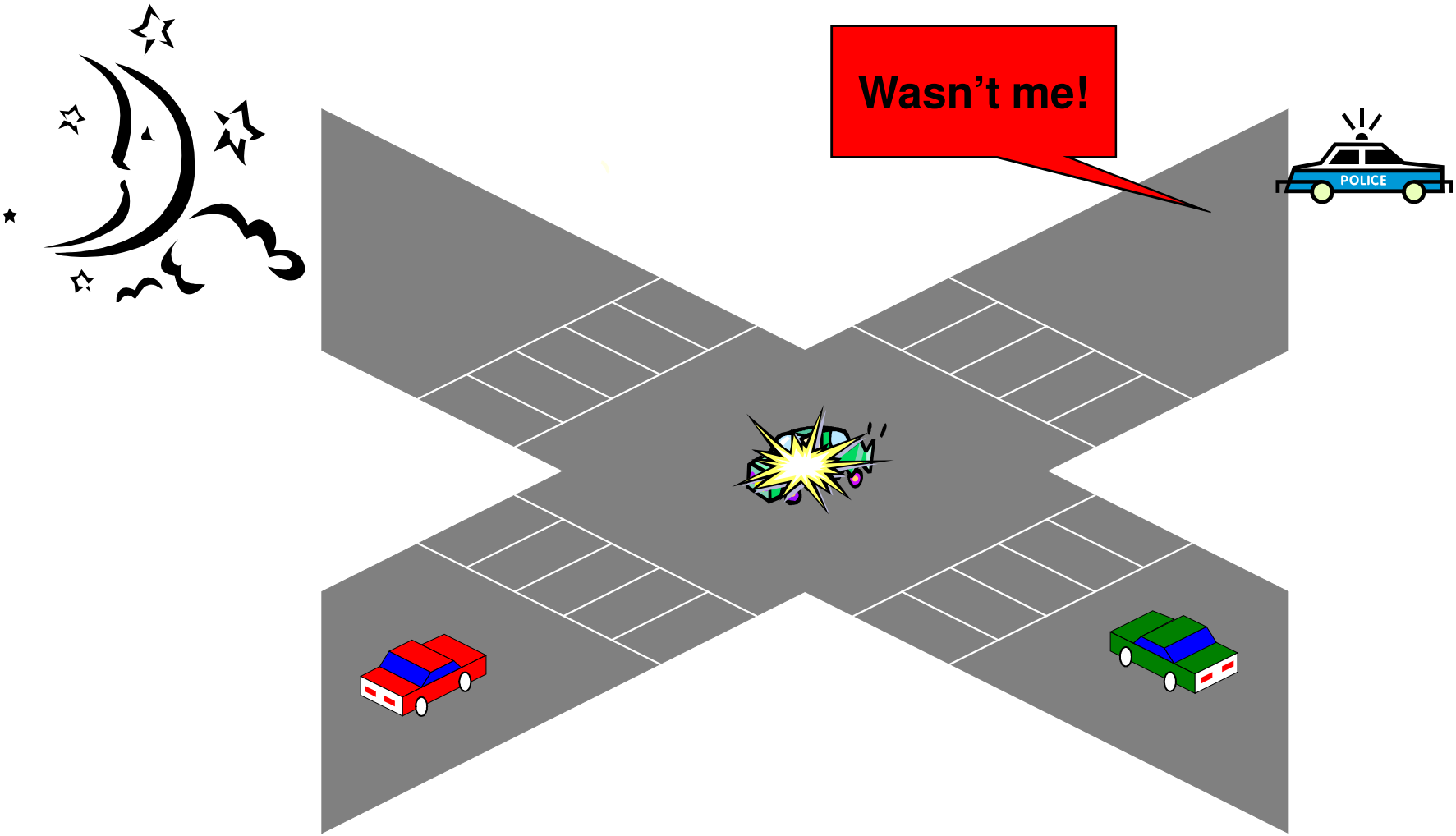


“Intelligent” Collisions





Cheating



Outline

- Classification of Cyber attackers
- Classification of attacks
- Cyber attacks against WSN
- Cyber attacks against VANET
- Cyber attacks against Intra-Vehicle Communications
- Classification of the Security Functions

Vulnerability Resume

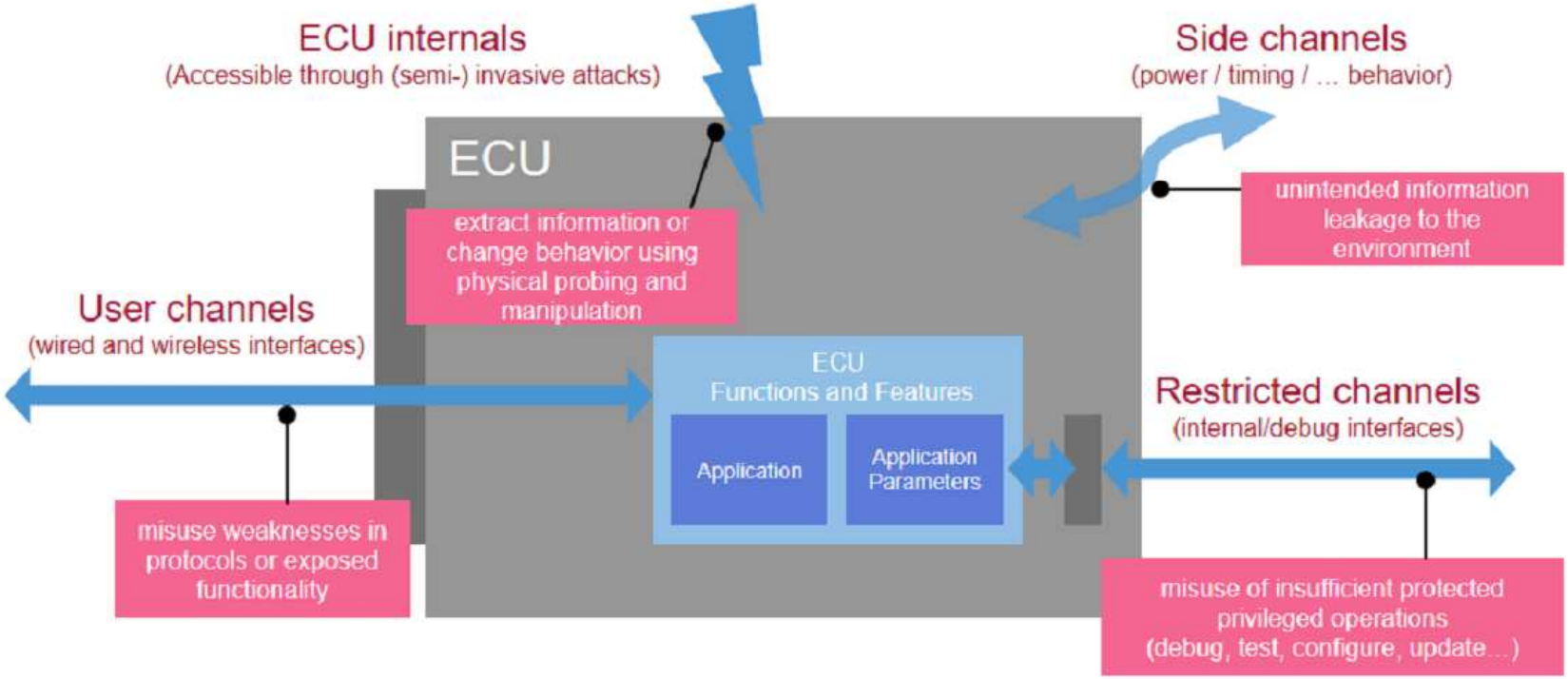
- Exchange of unciphered / unauthenticated messages
- Access to ECUs
- HW packaging

Attacks to Intra-Vehicle Communications

- **Eavesdropping**: any message is plaintext and the destination is not specified (any device has internal rules to determine if itself is the final destination of messages listened on the bus), therfore passive attackers can easily eaverdrop all communications.
- **Node Impersonation**: as neither authentication functions or explicit addressing mechnisms are foreseen, attackers can hijack devices and inject illegitimate messages.
- **Common Point of Entry**: any attack is pervasive on all the ECUs as a common gateway is used to connect the various communication buses (e.g. the port for diagnostics).
- **DOS**: communications are severely hindered through the manipulation of the system clock that regulates the sync timing in synchronous schemes or through the alteration of the arbitration mechanism for medium access in asynchronous schemes.

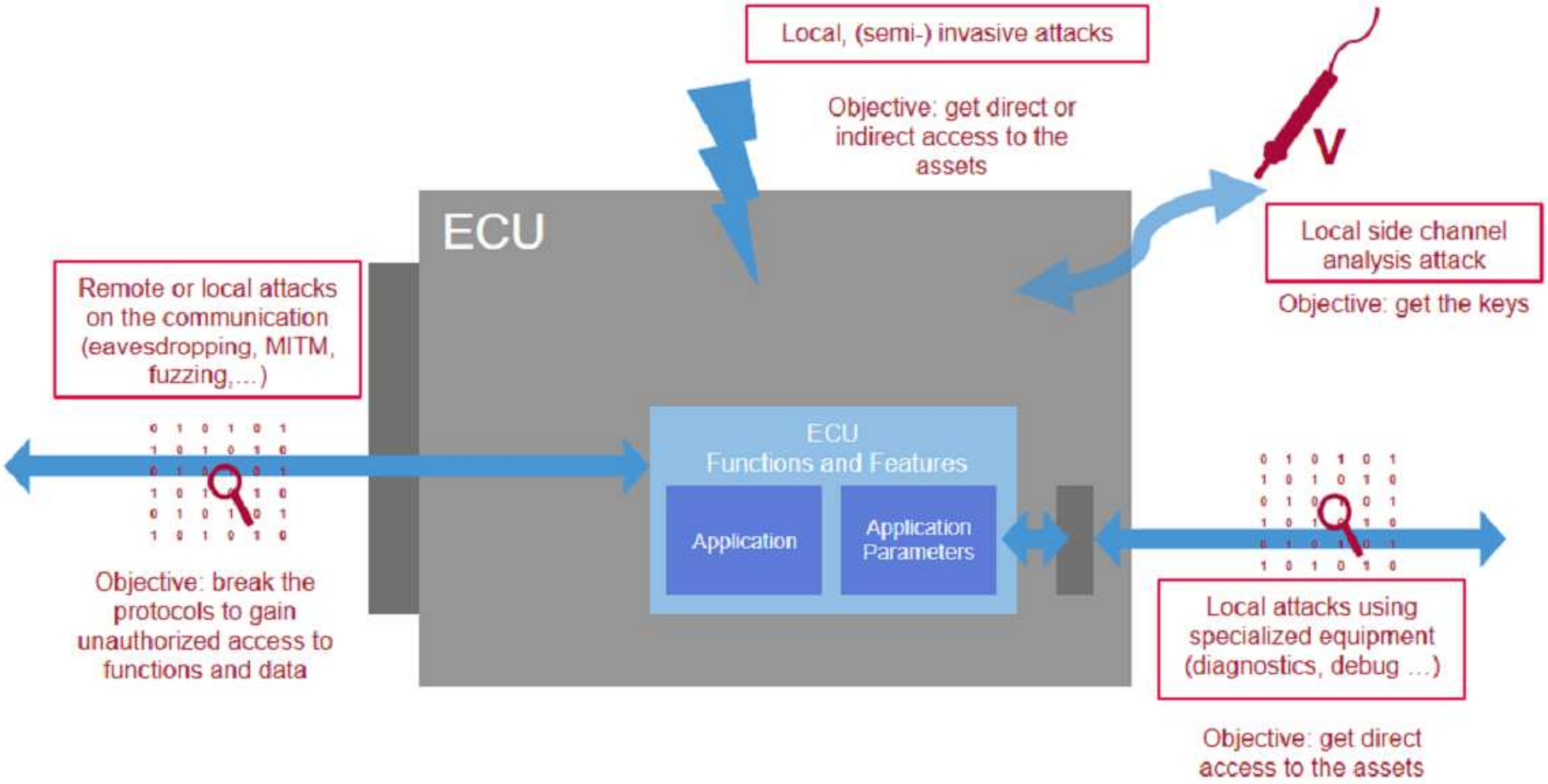
Attacks to ECUs

- The attack surface of ECUs is larger than only the interfaces. Information can also leak via unintended channels, typically called **“side channels”, that can be used to observe the internal behavior of the ECU or a component of it**. Typical state of art side channel attacks include Timing Analysis, Static / Dynamic Power Analysis (SPA/DPA), electromagnetic analysis (EMA) and photo-emission analysis.



Attacks to ECUs

- Attackers will, generally, use attack vectors that take the "path of least resistance" to achieve their objectives.



Outline

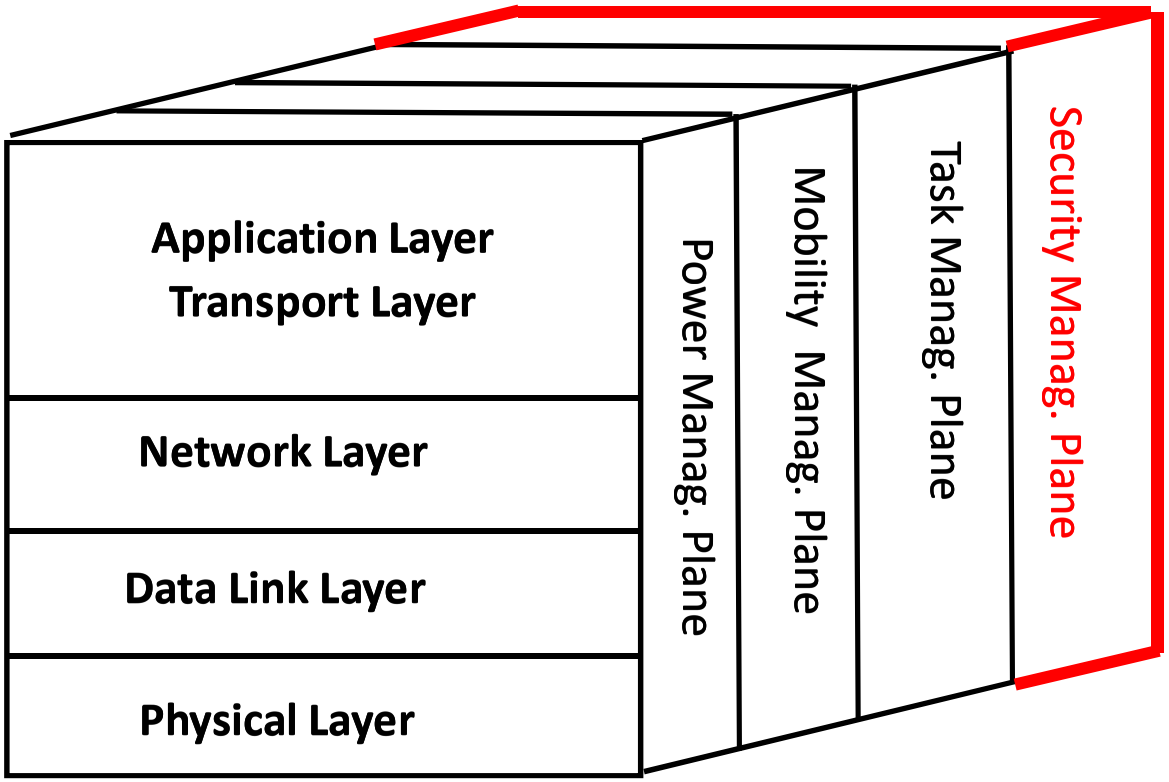
- Classification of Cyber attackers
- Classification of attacks
- Cyber attacks against WSN
- Cyber attacks against VANET
- Cyber attacks against Intra-Vehicle Communications
- Classification of the Security Functions

Security Management Plane

A “Security Management Plane” can be added to the reference protocol stack

- Power management plane
  - Manage duty cycles of active components.
- Mobility management plane
  - Detects and registers the movement of the nodes.
- Task management plane
  - Balances and schedules the sensing functions.
- Security Management Plane
  - Passive and Active Security Functions (PSF / ASF) to provide the required security to all functions in the reference protocol stack

Security Management Plane



Passive / Active Security Functions

- **Authentication**: PSF that ensures the sender identity of information can be verified by the receiver. Two kinds of authentications: information source (Sender Authentication) and information content (Integrity Authentication).
- **Integrity**: PSF that ensures information cannot be altered by unauthorized users (Integrity Authentication).
- **Confidentiality**: PSF that ensures information is unaccessible to unauthorized users.
- **Availability**: PSF that ensures information is can be always accessed by authorized users. Availability is related to system resilience and operation continuity.
- **Non-repudiation**: PSF that prevents a sender from transmitting information and from denying having done so. Furthermore, when a party A receives a false message from the party B, A can use the received information to accuse B for its forgery and convince the other nodes that B is a malicious node. Non-repudiation is related to accountability.
- **Traceability**: PSF that binds information to its sender. Traceability is related to accountability (e.g. in case of car accident) and non-repudiation. It is essential for VANET services.
- **Forward Secrecy:** capability of a PSF to protect past sessions against future compromises of secret keys (use of ephemeral keys)
- **Backward Secrecy:** capability of a PSF to protect future sessions against past compromises of secret keys

Passive / Active Security Functions

- **Authorization**: ASF that authorizes the access to resources or to a subsystem according to predefined authorization profiles (write / read) to computational resources, stored information, subnets and intercommunication channels in the subsystem (e.g. in VANETs, the intravehicular information exchanged by ECUs through an internal CAN bus). Therefore, authorization realizes a partial or total "logical segregation" between subsystems.
- **Intrusion Detection:** ASF that issues real time alerts when the system behavior is deviating (or getting anomalous) respect to a predefined behaviour (Anomaly Detection System, ADS)
  - AD is an algorithm to estimate system behavior and to to classify anomalies. Information from the system state is used to apply (dynamic) measures through actuators to fight the threat. Typically:
    - **IDS** to apply measures against induced misfunctioning
    - MS (Monitoring System) to apply measures against “natural” malfunctioning

- **Privacy**: mechanism that ensures the anonymization of a human when sensitive information about him is transmitted (GDPR).
  - The relation identity – pseudonym allows the direct privacy preserving operation.
  - The reverse relation pseudonym – identity with Traceability allows to get the real identity again as well as the overall dynamic of a specific occurrence.