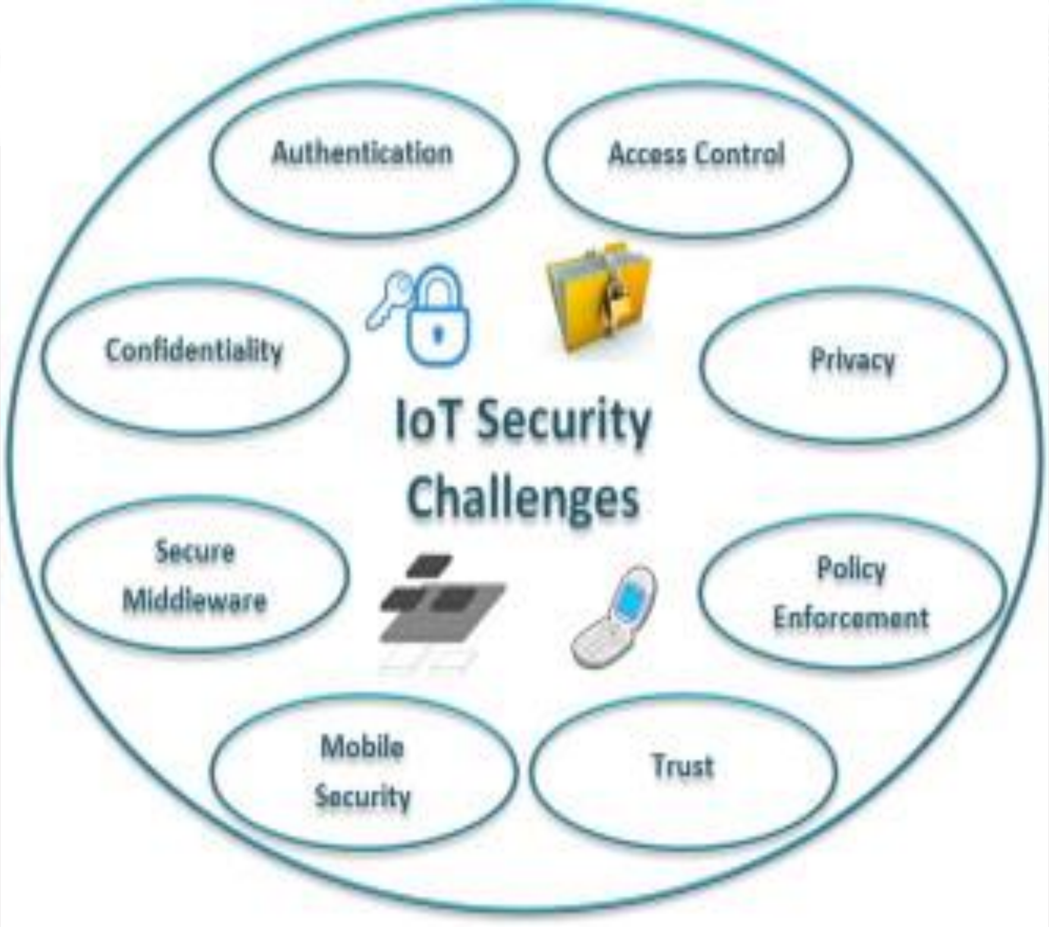


Cyber Physical Systems (IoT) Security

Henry Hexmoor, PhD

April 12, 2019

ForenSecure 2019

Chicago, IL,

USA

Southern Illinois University CARBONDALE

Henry Hexmoor Academic Bio

- PhD (Computer Science): SUNY Buffalo, 1995
- Dissertation: Cognitive processes involving *routine* activities
- MS+: 1982-1986 Robotics, Control theory, Philosophy.
- BS+: 1979-1982 Engineering (ME, EE, IE) plus Psychology and Social Sciences…

Robotics

NASA/Boeing Crystal Growth: GSFC

NASA Astronaut Helper: JSC   Robot kits…

Multiagent SystemsUSAF/SNC   Man on the loop

Trust networks;

Interrogational Policies;

Crowd Modeling

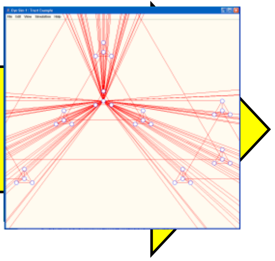
…

Network Science

Trait/Viral Injections

Online, Computational Organizations

Social Capital



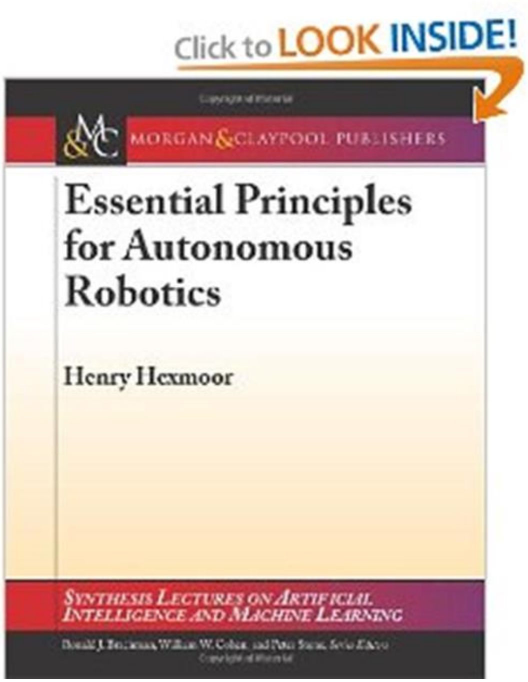
Complex Networks

Vehicular Platoons, Forensics

1995   2000   2005   2010   2015   2015

2020

Robotics, Automaton, and Network Science


Click to LOOK INSIDE!

Copyright of Material

MORGAN & CLAYPOOL PUBLISHERS

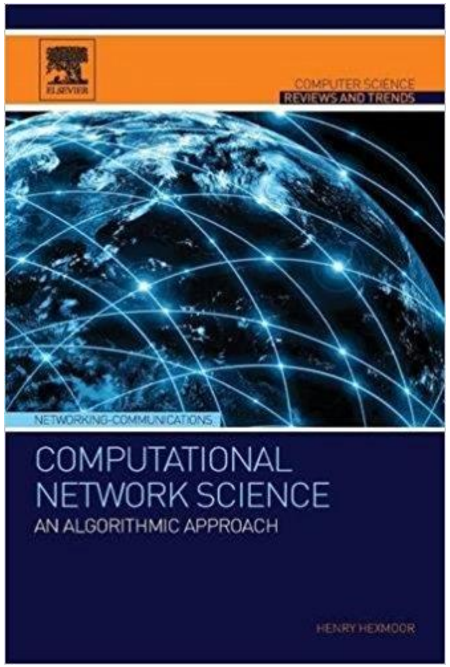
Essential Principles for Autonomous Robotics

Henry Hexmoor

SYNTHESIS LECTURES ON ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING

Ronald J. Brachman, William W. Cohen, and Peter Stone, Series Editors

Copyright of Material


ELSEVIER

COMPUTER SCIENCE REVIEWS AND TRENDS

NETWORKING-COMMUNICATIONS

COMPUTATIONAL NETWORK SCIENCE

AN ALGORITHMIC APPROACH

HENRY HEXMOOR

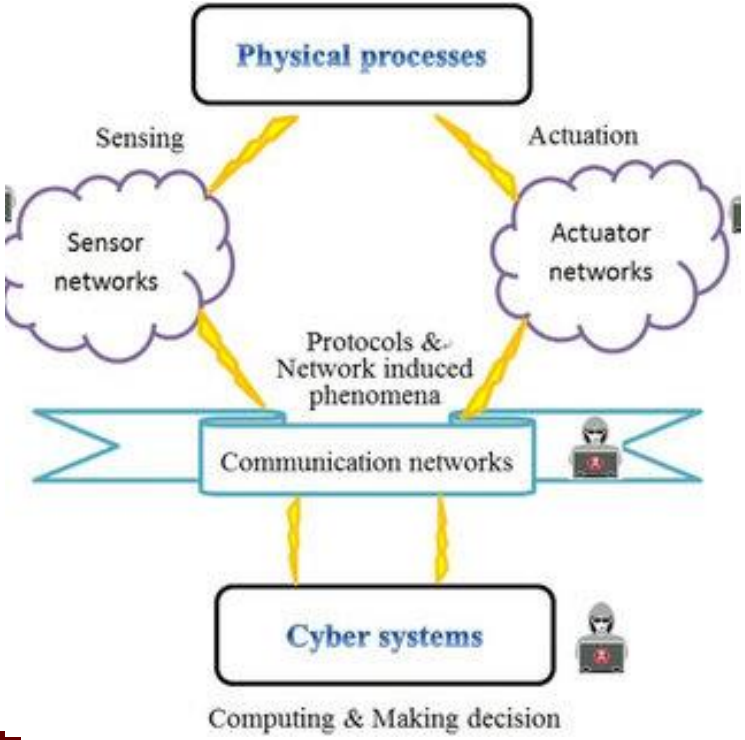
Outline

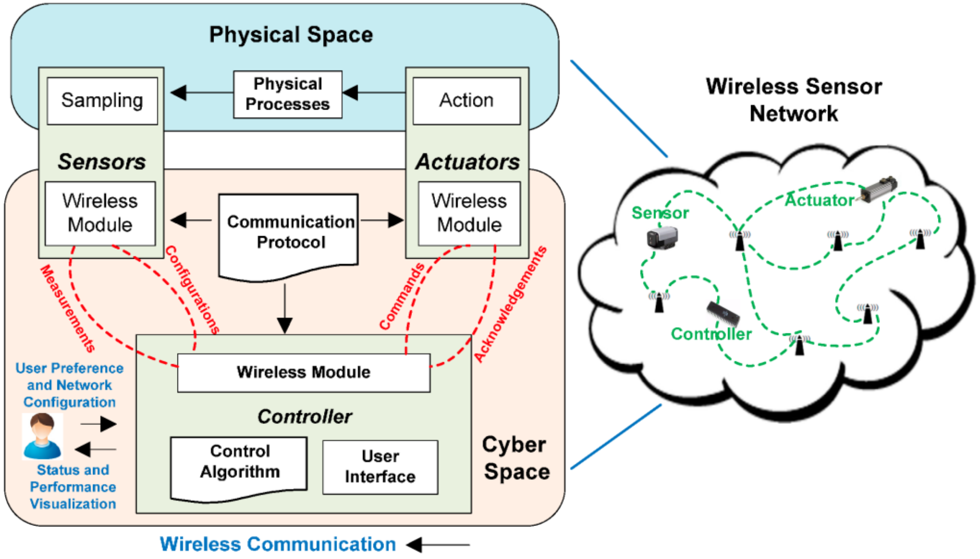
- Cyber Physical Systems/IoT
- The standard Security Tenets
- Malware
- Data Privacy & Trust
- Vehicular Security

©Henry Hexmoor

Cyber Physical Systems

- CPS (i.e., internet of things— IoT) is a large-scale, geographically dispersed, federated, heterogeneous, and critical systems with embedded devices such as sensors and actuators, networked to sense, monitor, and control the physical world.
- The Cyber component of CPS is a set of data transmitted among a set of Cyber-interconnected sensors, controllers, and actuators.





Basic Features of CPS/IoT

- IoT are emerging to a large number of nodes that are collectively pervasive.
- With minimal human intervention, objects in the IoT are performing data collection, processing, collaborating with each other, and decision-making in an autonomous fashion.
- They support different wireless communication technologies (such as Bluetooth low energy (BLE), Global System for Mobile Communications (GSM), near field communication (NFC), Wi-Fi, and interdependently operate between the cyber and the physical world.
- With various radio interfaces, objects can communicate with each other in more complicated ways, forming a complex network.
- For example, an object may communicate with another object via a GSM interface over cellular networks, while also communicating with a different object in the geographic vicinity via proximity-based communication technologies using Bluetooth Low Energy (BLE), Wi-Fi Direct, etc.

Standard Tenets of Security (1/2)

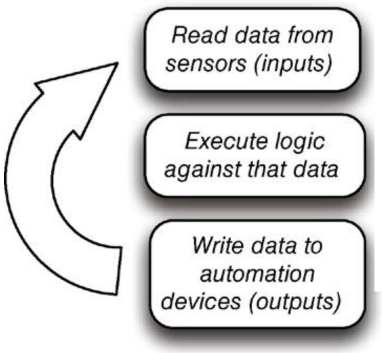
- Threat: a set of circumstances that has the potential to cause loss or Harm.
  - The loss might be in safety measures including confidentiality, integrity, or availability of resources, whereas the harm implies hurting people, the environment, or systems. Threat types:
    a. adversarial threats
    b. accidental threats
    c. environmental threats
    d. failures of supporting infrastructure (e.g., power or telecommunications outages)
- Vulnerability: possibility of exposure to attacks
  - Cyber — communication between CPS and the external world
  - cyber-physical — communication among CPS components
  - physical vulnerabilities — kinetic exposure
  - Reliance on open standards protocols, such as TCP/IP
  - Remote procedure calls (e.g., Stuxnet attack)
  - SQL injection is a web-related database records access without authorization
  - Untrusted devices connecting to local networks and adding malicious code.

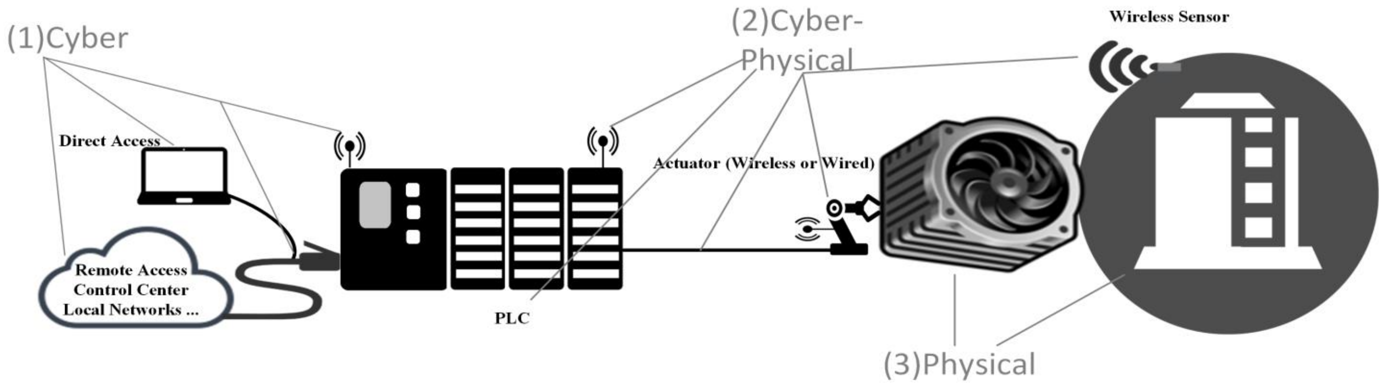
Standard Tenets of Security (2/2)

- Attack:
  - CPS attackers have one or more reasons to launch an attack: criminal, spying, terroristic, political, or cyberwar
- Control:
  - Secure the access point from unauthorized access.
  - Intrusion Detection Systems (IDS) should be time-critical so that long delays are intolerable.
  - Software need to verify the software's authenticity, i.e., device attestation.
  - Only authorized personnel can remotely access field devices.
  - Access should be strictly secured by using a designated laptop through a VPN.

Industrial scale CPS

- Industrial Control Systems (ICS) are the control systems to enhance control, monitoring, and production in industries such as the nuclear plants, water and sewage systems, and irrigation systems.
- ICS is also called Supervisory Control and Data Acquisition (SCADA) or Distributed Control Systems (DCS).
- Programmable Logic Controller (PLC) is a microprocessor device designed to operate continuously in hostile environments that is equipped with wireless and wired communication capacity. PLC typically control real-time processes, and so they are designed for simple efficiency. The logic used in PLCs is typically very simple and is programmed according to an international standard set of languages.
- It is possible to capture packets and simply replay them to inject a desired command into the system because most industrial control traffic is transmitted in plain text.
- The smart grid is envisioned updated grid for electricity generation, transmission, and distribution.


Read data from sensors (inputs)
Execute logic against that data
Write data to automation devices (outputs)

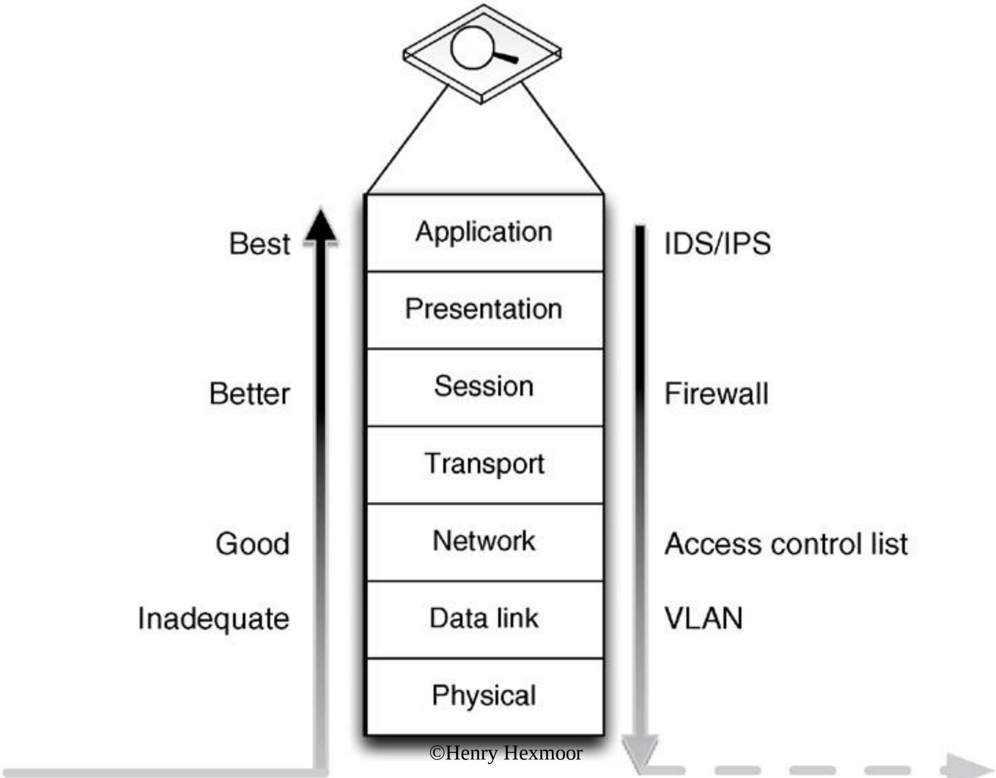

(1)Cyber
(2)Cyber-Physical
Wireless Sensor
Direct Access
Actuator (Wireless or Wired)
Remote Access Control Center Local Networks ...
PLC
(3)Physical

Active Versus Passive Attacks

- A passive threat is performed only by eavesdropping through communication channels or the network.
- In active threats, the attacker is not only skillful in eavesdropping on communication channels, but also in modifying IoT systems to change configurations, control communication, deny services, etc.
- Attacks may include a sequence of interventions, disruptions and modifications.
  - For example, potential attacks on an IoT system may involve impersonation (e.g. spoofing, Sybil and man-in-the-middle), malicious inputs, data tampering and DoS.

Attack Monitoring

- Application-layer session monitoring provides a valuable and necessary level of assurance, as it is able to detect low-level protocol anomalies and application policy violations (such as an unauthorized attempt to write a new configuration to a PLC).
- The most stringent network security device may be the data diode, also referred to as a unidirectional gateway.



©Henry Hexmoor

Attacks a different OSI Layers

Application Layer

User authentication

Data Tampering

Transport Layer

DoS DDOS

Man in the moddle

Masquerade

Network Layer

Routing Protocols

Address Compromise

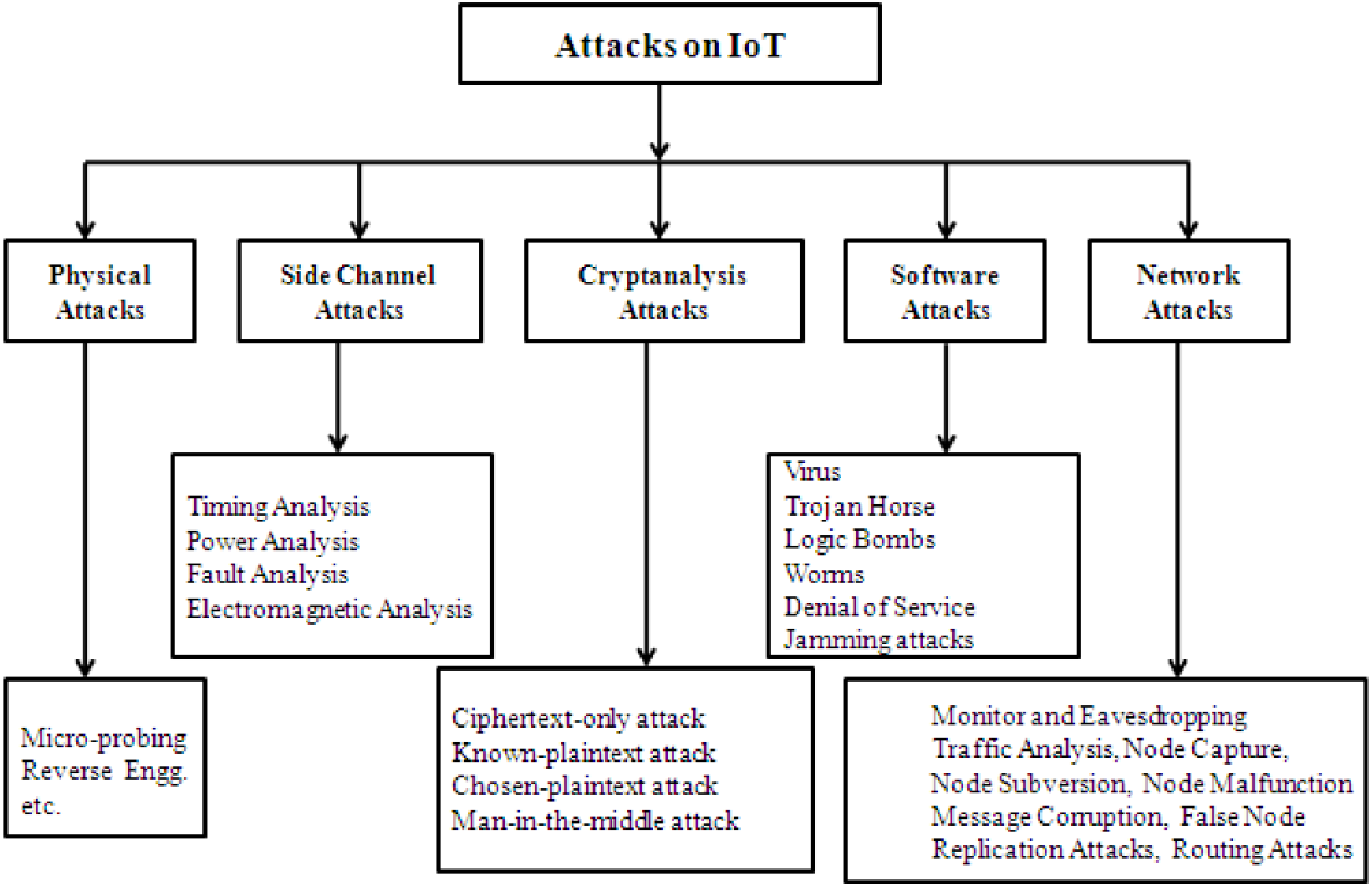
Sensing and Perception Layer Attacks

Access control: Brute Force User Credentials-- Keyloggers, Trojans, Network sniffing

Wormhole, Sewage pool, Witch, HELLO flooding, Sewage pool,

Selective forwarding, link layer, …

Summary of known IoT attack Types



Attacks on IoT

Physical Attacks

Micro-probing
Reverse Engg.
etc.

Side Channel Attacks

Timing Analysis
Power Analysis
Fault Analysis
Electromagnetic Analysis

Cryptanalysis Attacks

Ciphertext-only attack
Known-plaintext attack
Chosen-plaintext attack
Man-in-the-middle attack

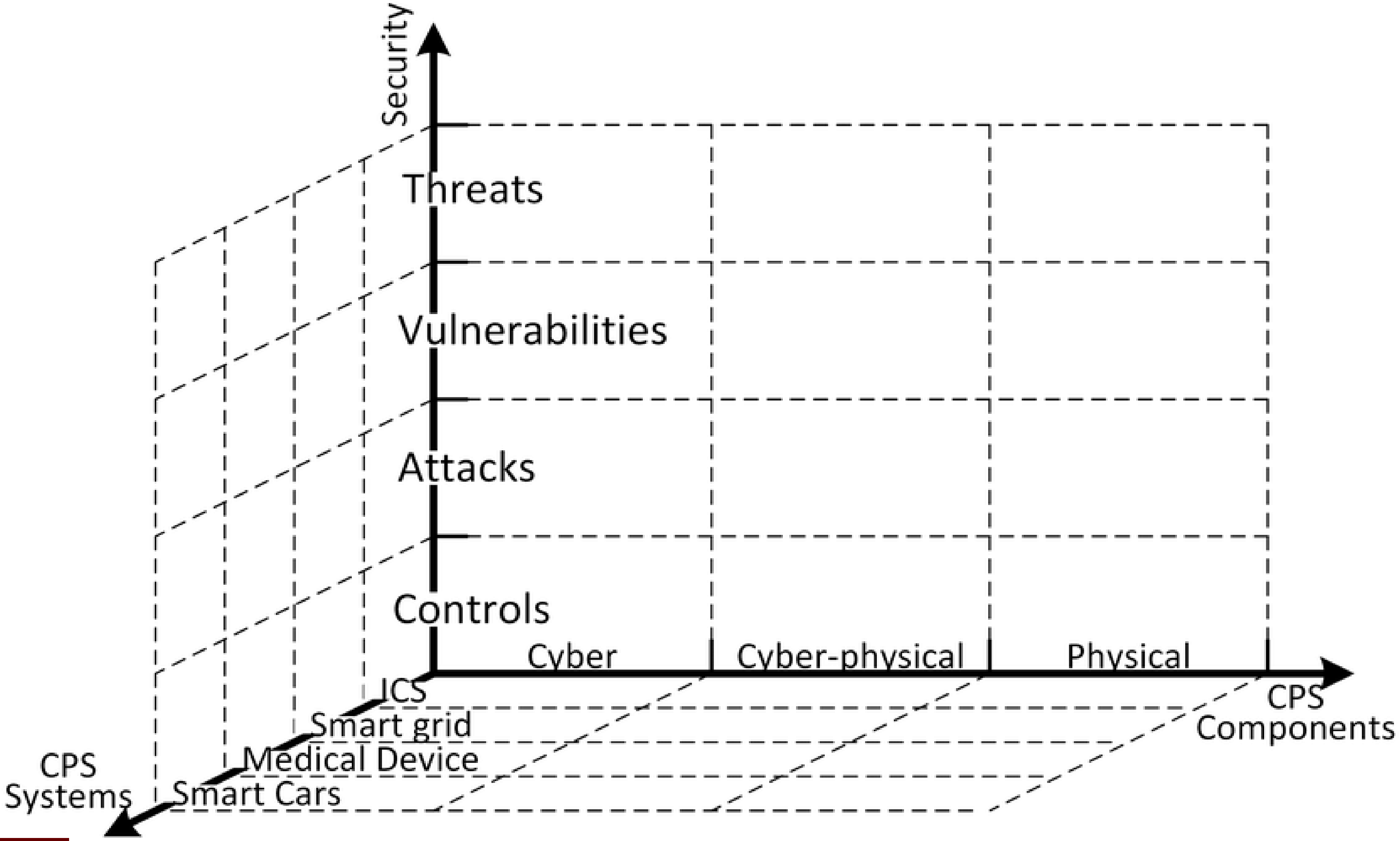
Software Attacks

Virus
Trojan Horse
Logic Bombs
Worms
Denial of Service
Jamming attacks

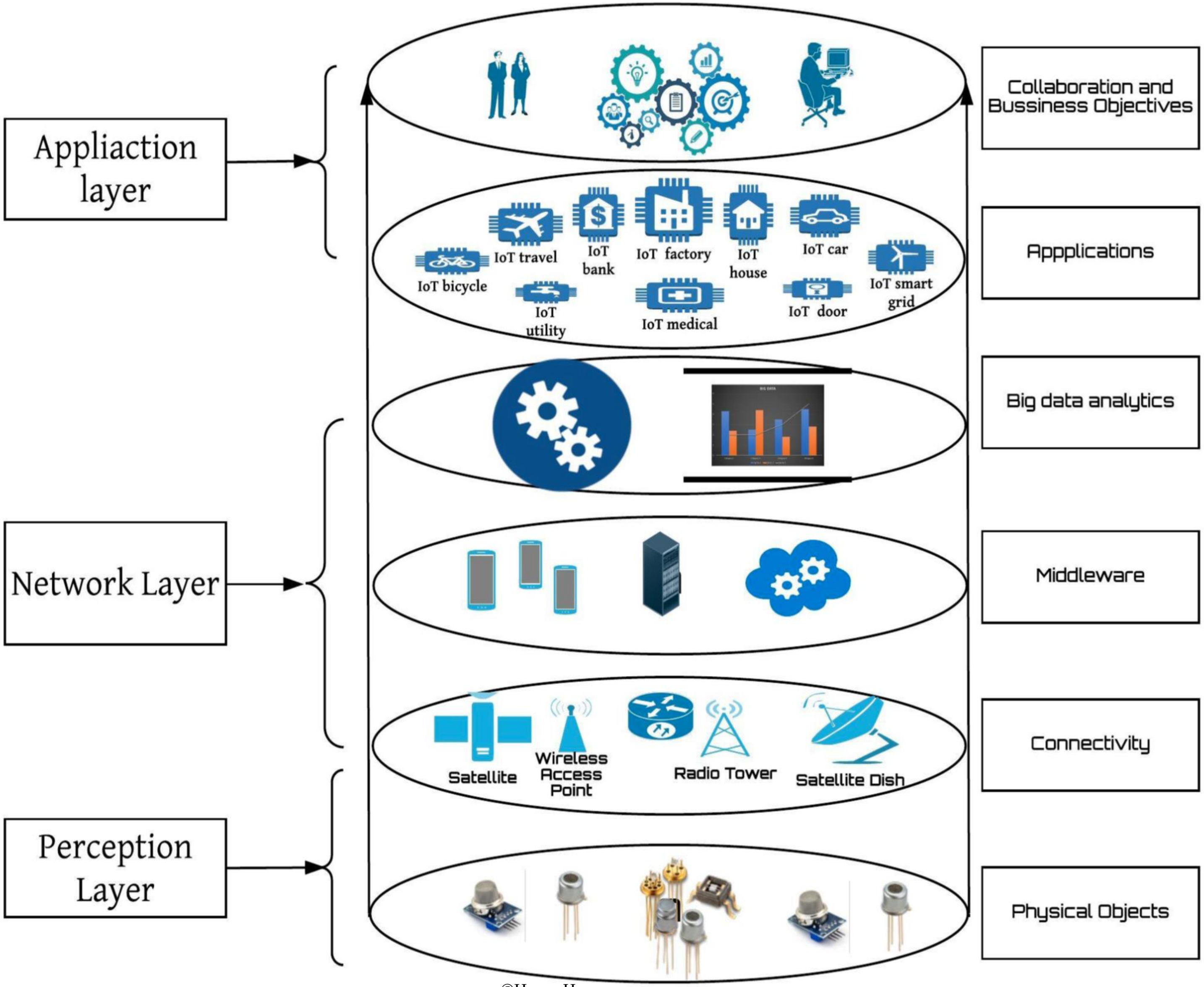
Network Attacks

Monitor and Eavesdropping
Traffic Analysis, Node Capture,
Node Subversion, Node Malfunction
Message Corruption, False Node
Replication Attacks, Routing Attacks

Three orthogonal coordinates…



IoT Layers



Appliaction layer

Network Layer

Perception Layer

Collaboration and Bussiness Objectives

Appplications

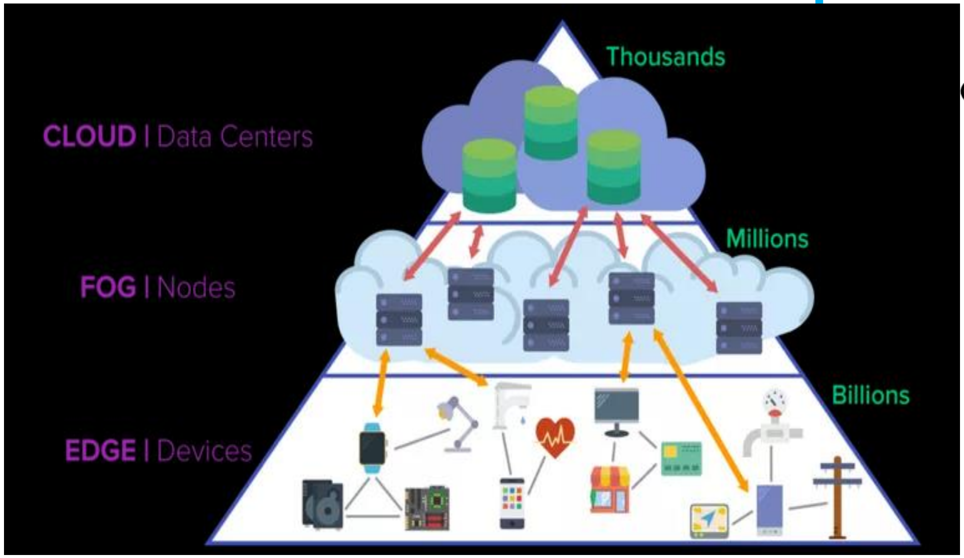
Big data analytics

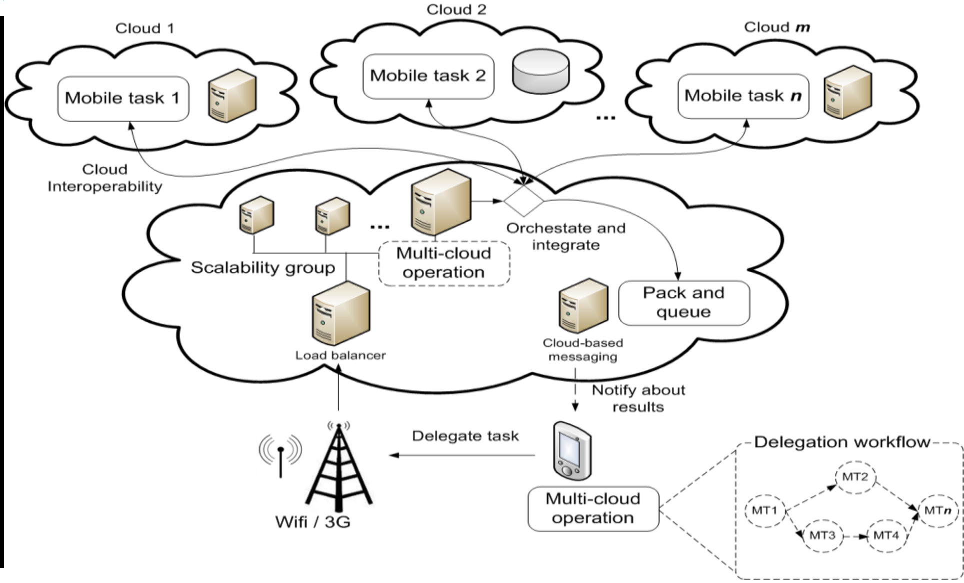
Middleware

Connectivity

Physical Objects

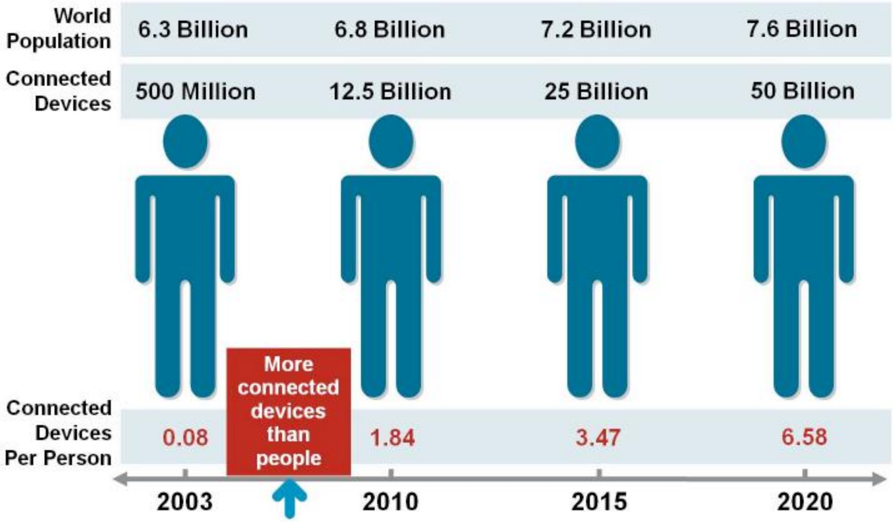
Mobile task Delegation of resource-intensive operations





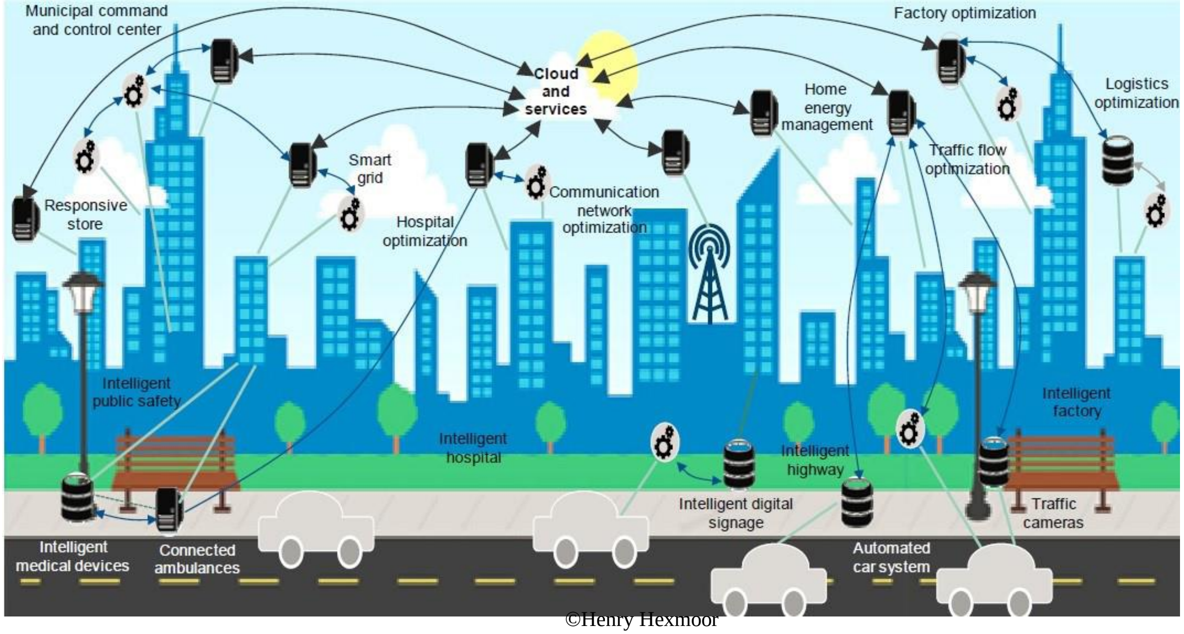
Smart Grid
Automated Lighting
Pool Sensor
Smart Appliances
Smart Thermostat
Garage Door Opener
Security System
Gas/Water Meter
Smart e-meter
WLAN/HAN Gateway
Sprinkler System

Mobile task Delegation of resource-intensive operations



	2003	2010	2015	2020
World Population	6.3 Billion	6.8 Billion	7.2 Billion	7.6 Billion
Connected Devices	500 Million	12.5 Billion	25 Billion	50 Billion
Connected Devices Per Person	0.08	1.84	3.47	6.58

More connected devices than people



CPS/IoT Vulnerabilities to Malware

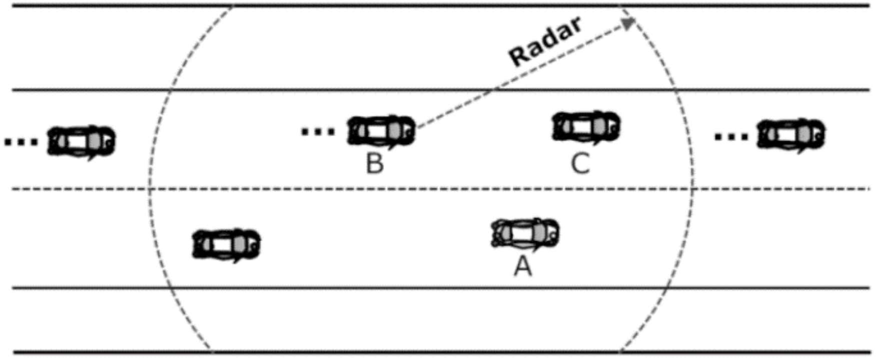
- Due to the nature of the limitations of computing capability and energy, the algorithm and mechanism applied to the object are relatively simple.
- Conventional security mechanisms such as real-time antivirus scanning cannot be used for the IoT platform due to the unaffordable overhead.
- Attackers can spend much less resource to break in, and thus, the object becomes a target of malicious users. Another good example is the limited logging, which makes the identification of intrusion harder.
- The large number of objects with various, heterogeneous actions and behaviors enables fabrication of identity.
- The mix of infrastructure-based and proximity-based communication technologies causes malware to propagate rapidly.
- Malware propagate via infrastructure-based communication technologies such as GSM/General Packet Radio Service (GPRS)/Universal mobile telecommunications System (UMTS)/Long-Term Evolution (LTE) and wireless local area network (WLAN).
- Alternatively, Using proximity schemes BLE, Wi-Fi direct, and NFC, attackers infect the objects in the vicinity and cause an epidemic spread.

Mitigating Malware

1. Using a global timer for data expiration, the infected nodes delete the data, and therefore the nodes transit from the infected state to the recovered state.
2. A recovered node participates in vaccinating the susceptible nodes against the malware. A susceptible node becomes a vaccinee and is therefore immune to the epidemic.

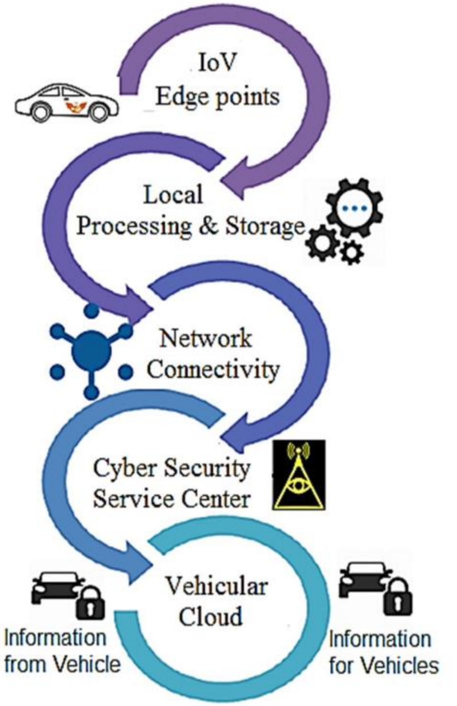
Vehicular Sybil Attack

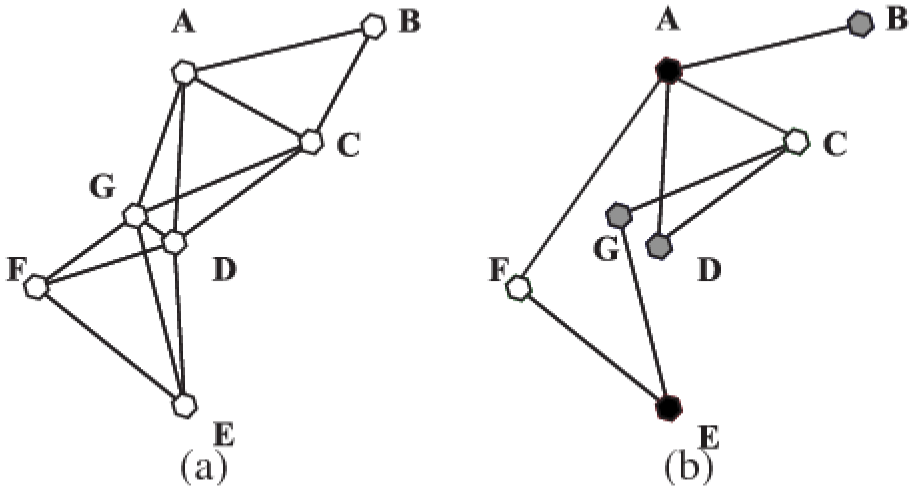
- An attacker tries to violate the unique vehicular ID property by forging or fabricating it and presenting multiple identities. It results in large-scale denial of service or other security risks in the network.
- The Sybil attack affects the performance of geographical routing and leads to large-scale denial of service.
- Reputation and trust management system crucially depend upon the unique ID and authenticity of the node. A Sybil attack violates this assumption and results in erroneous computation of reputation values.
- A Sybil node will have with multiple identities and can manipulate sensor aggregate values resulting in misleading aggregate values.
- A Sybil attack can be prevented by using public key certificates issued by a central authority (CA).
- A distributed approach is for RSUs to acts as authority to verify the authenticity of a vehicle node by using the information consensus from nearby RSUs.



Data Privacy

- The Spatial Privacy Graph identifies the privacy pairs that should select different storage nodes to save their data.
- Map each storage node to a unique color numbered from 1 to n.
- Each sensor node assigns its color purely based on its neighbors' colors.
- A pair of nodes are neighbors if they are connected in the SPG.





Trust Based Authentication

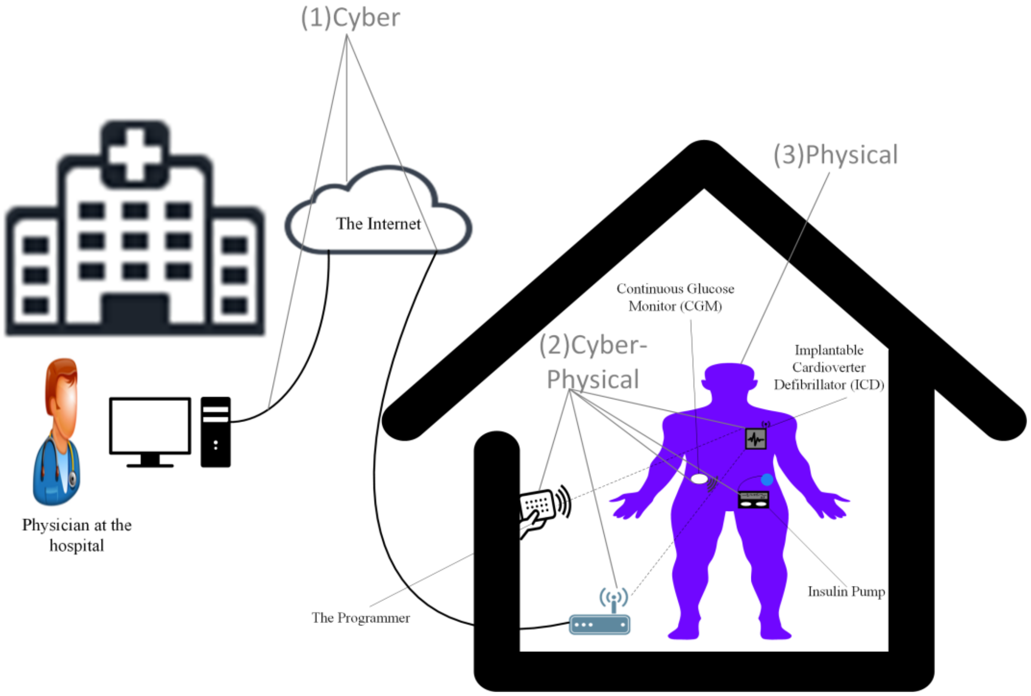
- Secure storage facilities (also known as keystores) increase the robustness of trust tokens used both within an IoT system.
- Passive keystores provide a means to securely save and retrieve credentials; cryptographic operations are executed outside these stores by the device's CPU.
- Active keystores allow the internal execution of cryptographic operations via an application program interface (API), so the credentials are never exposed.
- During the operation of a network, devices set up static or dynamic shortlived communication links with other peers.
- Trust tokens are exchanged and validated, or new session tokens are created.
- In a direct trust model, a peer obtains credentials of other peers that it is convincing to them.
- In a web-of-trust model, peers accepts credentials of other peers if these credentials are validated (e.g., signed) by an already trusted peer.

Smart Grid Attacks

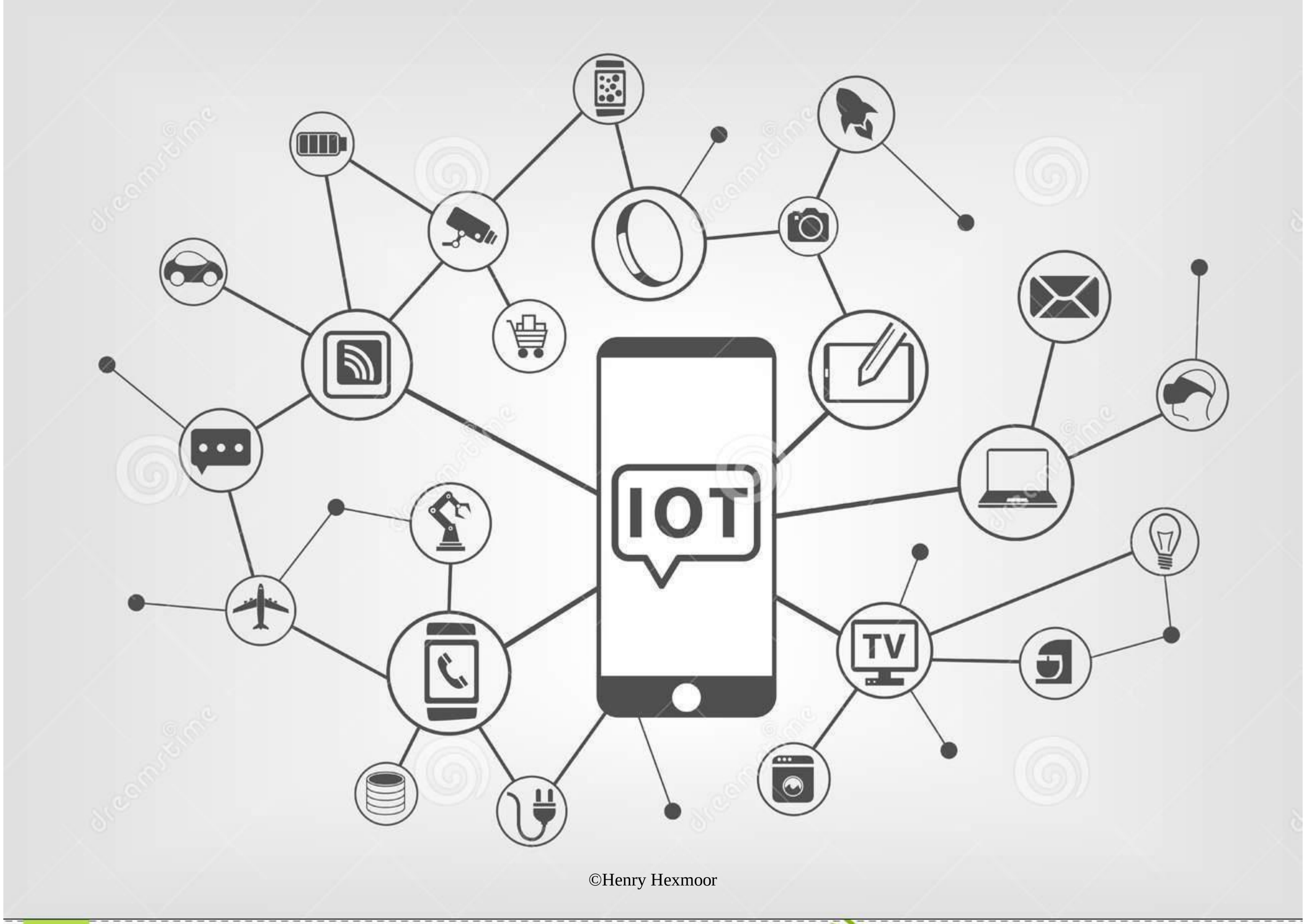
- Flooding the network at different layers is a possible approach to achieve DoS attacks.
- Introducing false data in smart grids' traffic leads to different consequences such as service disruption and financial losses.
- Attackers can analyze network traffic in smart grids between smart meters and data centers to infer private information about customers.
- The Slammer worm infected a nuclear plan in Ohio in 2003 resulted in disabling the traffic between field devices and substations.
- Blackouts

Medical Device Attacks

- By exploiting a vulnerability in an insulin pump, replaying eavesdropped packets is possible by incorporating a previously intercepted device’s PIN. Replay attacks could result in misinformed decisions regarding insulin injection


(1)Cyber
The Internet
(3)Physical
Continuous Glucose Monitor (CGM)
(2)Cyber-Physical
Implantable Cardioverter Defibrillator (ICD)
Physician at the hospital
Insulin Pump
The Programmer

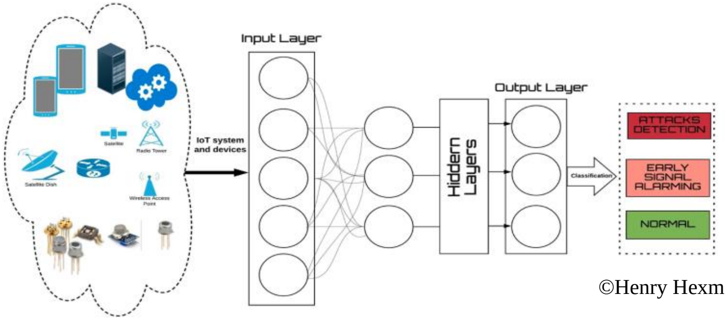
Smart Phones & IoT

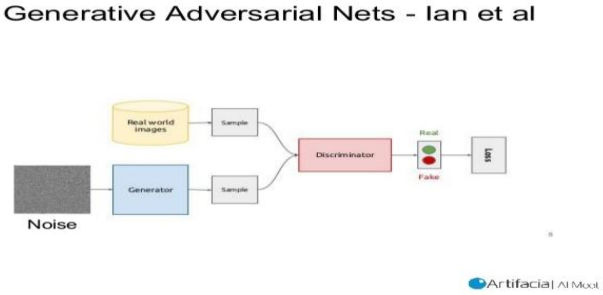


©Henry Hexmoor

Machine and Deep Learning

- Machine learning and deep learning (ML/DL) are methods of data exploration to learn about 'normal' and 'abnormal' behavior according to how IoT components and devices interact within the environment to support intrusion detection.
- Inspired by the working mechanisms of the human brain and neurons for processing signals, DL is a ML subfield that uses several non-linear processing layers for discriminative or generative feature abstraction and transformation for pattern analysis.
- Advantage of Deep Learning (DL) over traditional ML is its superior performance in large datasets.
- Generative adversarial networks (GANs) trains two models, namely, generative and discriminative models. GANs can be used to build an architecture for securing the cyberspace of IoT systems

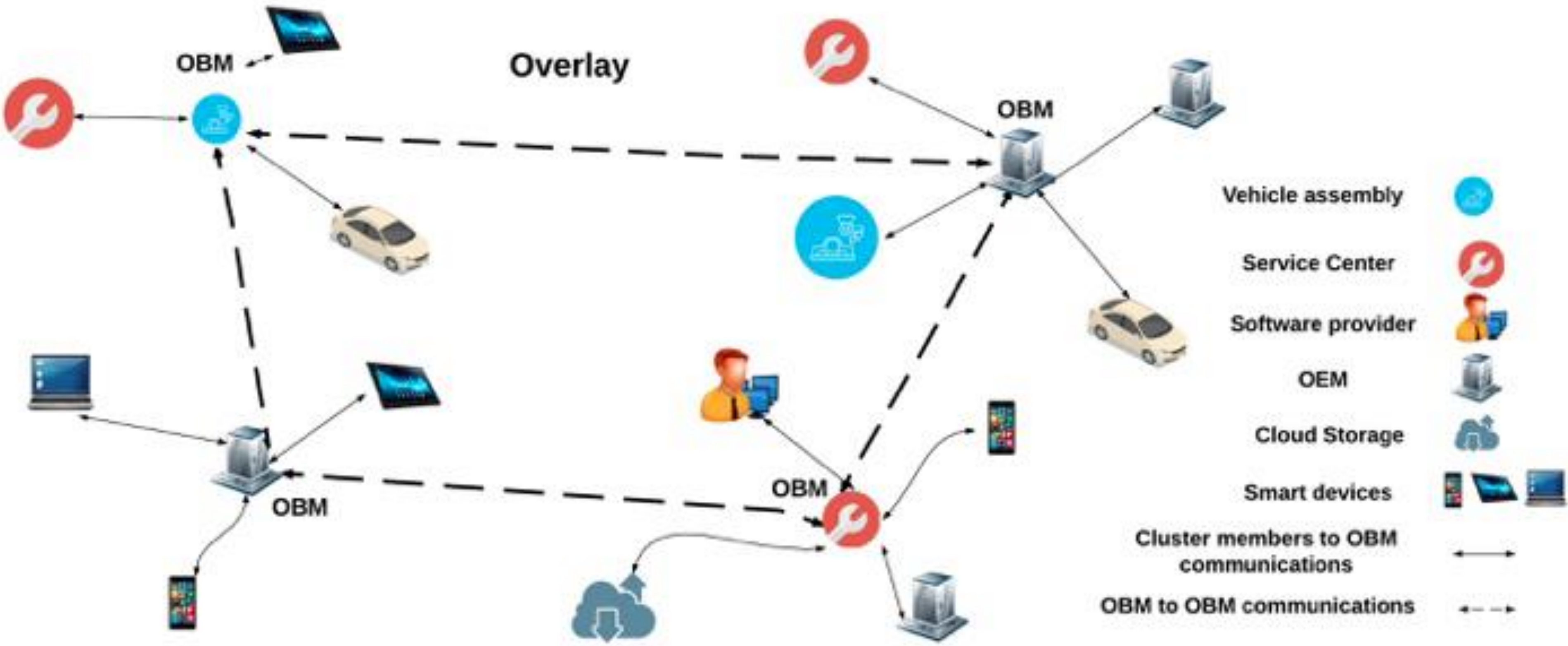




Distributed, BlockchainVehicle Authentication

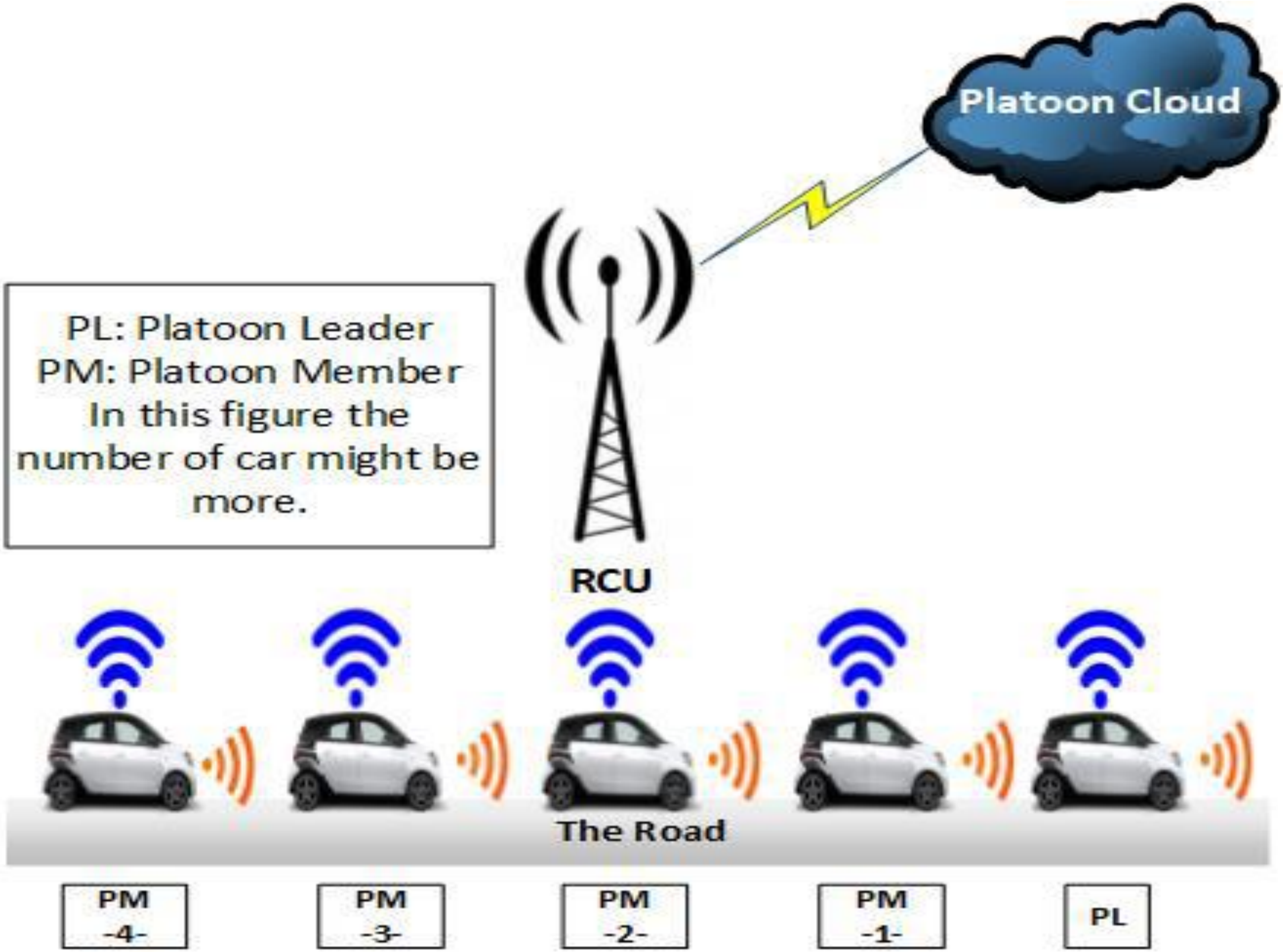
- A public blockchain is managed by the overlay nodes that are smart vehicles.
- Each vehicle is equipped with a Wireless Vehicle Interface (WVI) and local storage, such as a micro SD card. The WVI connects the vehicle to the overlay.
- The in-vehicle storage is used to store privacy sensitive data, e.g. location and maintenance history, to protect the privacy of the user. Vehicle generates single signature transactions in pre-defined time intervals containing the signed hash of the data stored in the in-vehicle storage.
- This transaction is sent to the Overlay block manager (OBM) that the vehicle is associated with and thus stored in the BC.
- At a later time, the vehicle can prove that the data within its storage has not being changed by verifying the hash contained in this transaction.
- As the in-vehicle storage has limited capacity, a back-up storage can be considered in the smart home of the vehicle owner.
- The vehicle periodically transfers data from the in-vehicle storage to the backup storage. In this instance, the hash of the backup storage is stored in the BC.
- Overlay transactions are broadcast and verified by the OBMs.
- An OBM verifies a transaction by validating the signature of the transaction participants with their PK.

Distributed, Vehicle Authentication

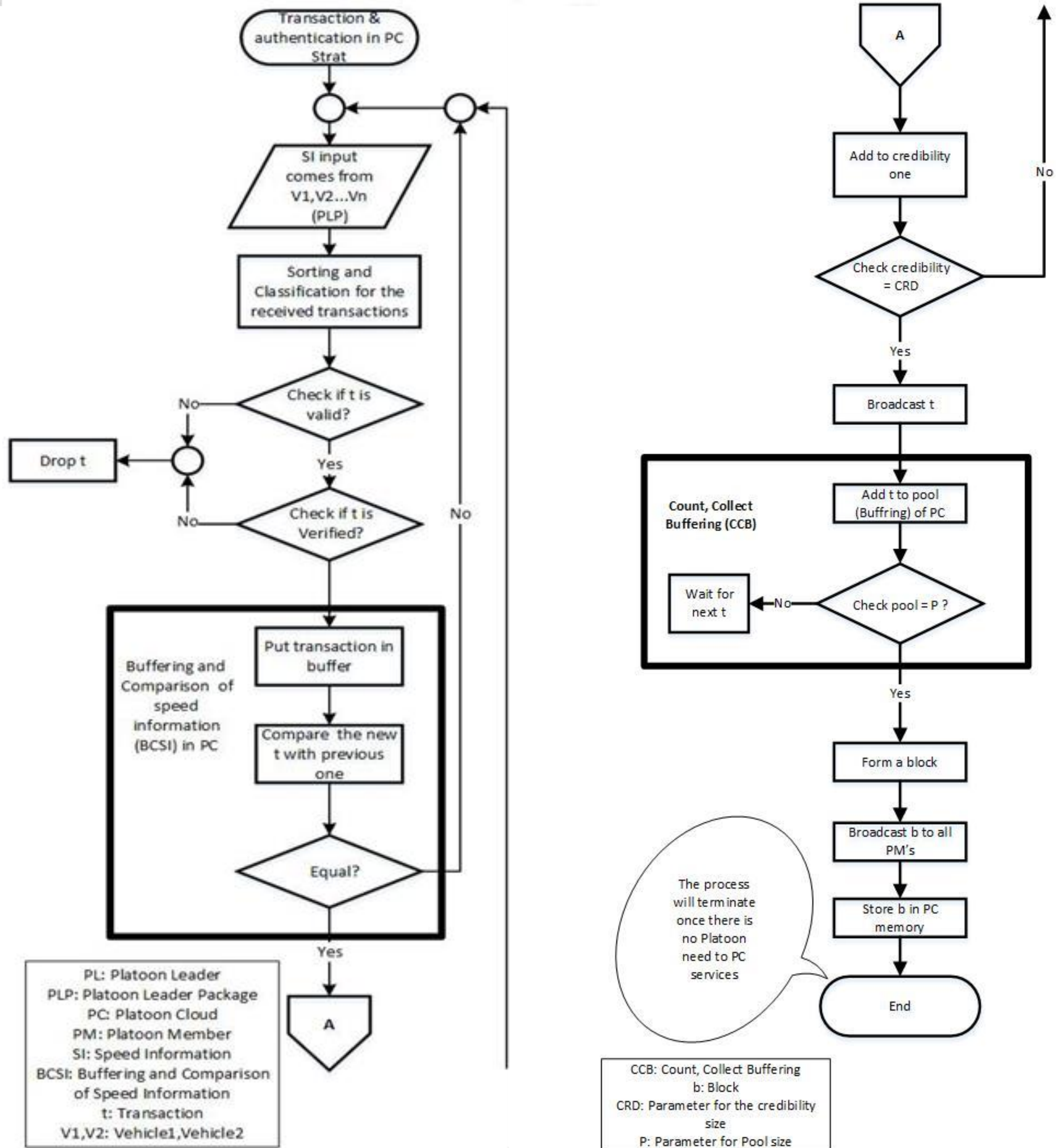


- Each node is known by a changeable PK.
- Changing the PK for each transaction introduces a high level of privacy. However, in some instances other nodes may need to identify the real-world identity of a PK owner, e.g. the vehicles.
- We need to know the PK of their OBM so that they can trust requests sent from the OBM.

Vehicle Platooning is an appication area



Blockchain Authentication



Transaction & authentication in PC Strat

SI input comes from V1,V2…Vn (PLP)

Sorting and Classification for the received transactions

Check if t is valid?

No

Yes

Drop t

Check if t is Verified?

No

No

Buffering and Comparison of speed information (BCSI) in PC

Put transaction in buffer

Compare the new t with previous one

Equal?

Yes

A

PL: Platoon Leader
PLP: Platoon Leader Package
PC: Platoon Cloud
PM: Platoon Member
SI: Speed Information
BCSI: Buffering and Comparison of Speed Information
t: Transaction
V1,V2: Vehicle1,Vehicle2

A

Add to credibility one

Check credibility = CRD

No

Yes

Broadcast t

Count, Collect Buffering (CCB)

Add t to pool (Buffring) of PC

Check pool = P ?

No

Wait for next t

Yes

Form a block

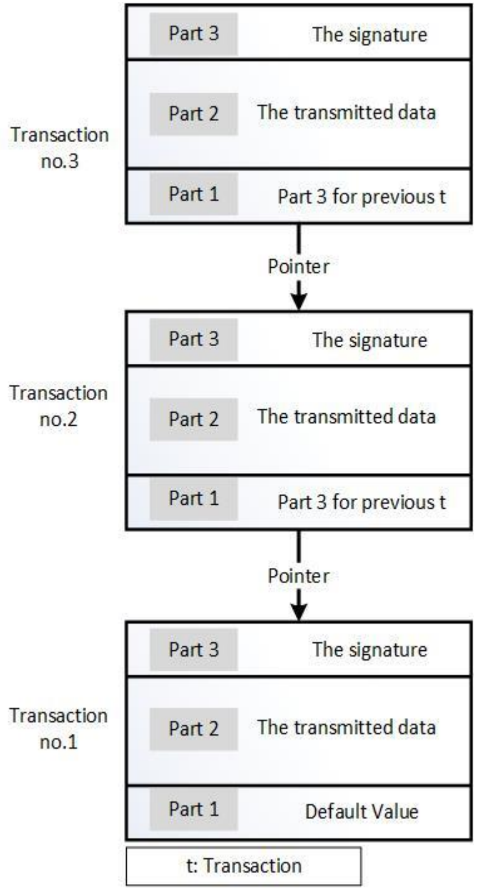
Broadcast b to all PM's

Store b in PC memory

End

The process will terminate once there is no Platoon need to PC services

CCB: Count, Collect Buffering
b: Block
CRD: Parameter for the credibility size
P: Parameter for Pool size



Transaction no.3

Part 3	The signature
Part 2	The transmitted data
Part 1	Part 3 for previous t

Pointer

Transaction no.2

Part 3	The signature
Part 2	The transmitted data
Part 1	Part 3 for previous t

Pointer

Transaction no.1

Part 3	The signature
Part 2	The transmitted data
Part 1	Default Value

t: Transaction

Common Blockchain Attacks

- An attacker can compromise an OBM and generate blocks with fake transactions to create false reputation.
- An OBM can detect a fake block during the verification step …
- An attacker can flood an overlay node (i.e., DOS of target) with a large number of transactions to overwhelm the node …
- OBMs would not send a transaction to their cluster members unless they find a match with an entity in their key list.
- Multiple overlay nodes or devices are compromised by the attacker.
- It is Possible that an attacker can introduce fake devices to the system to gain access to private information within the system.

The Center for Internet Security… Recommendations

1. **Deploy an automated asset inventory discovery tool** for inventory of systems. Use a mix of active and passive tools.
2. If the organization is dynamically assigning addresses using DHCP, **deploy dynamic host configuration protocol (DHCP) server logging**…
3. … **automatically update the inventory** system as new, approved devices are connected to the network.
4. **Maintain an asset inventory** …
5. **Deploy network level authentication …**
6. **Use client certificates to validate and authenticate** systems prior to connecting to the private network.

Follow ups…