Resilient RFID Grouping Proofs with Missing Tag Identification

Mike Burmester, Florida State University, FL, USA

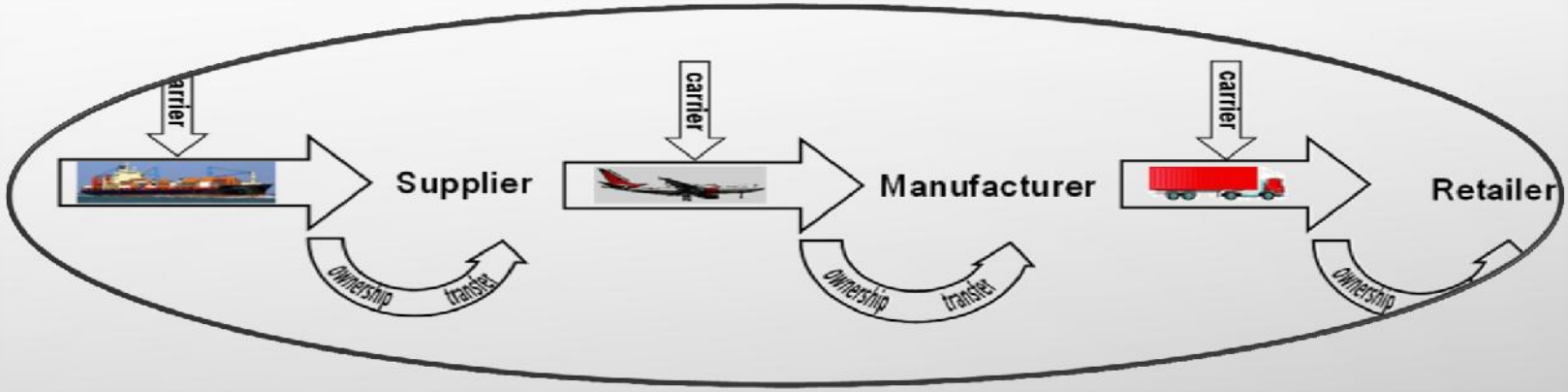
Jorge Munilla, Universidad de Malaga, Spain

10th Inter. Confer. Ubiquitous Computing & Ambient Intelligence UCAmI 2016

Canary Islands (Spain). Nov 29th to Dec 2nd, 2016

Contents

Introduction-Supply Chain



Goals for securing the supply chain

— promote efficient and secure services

— foster resilience

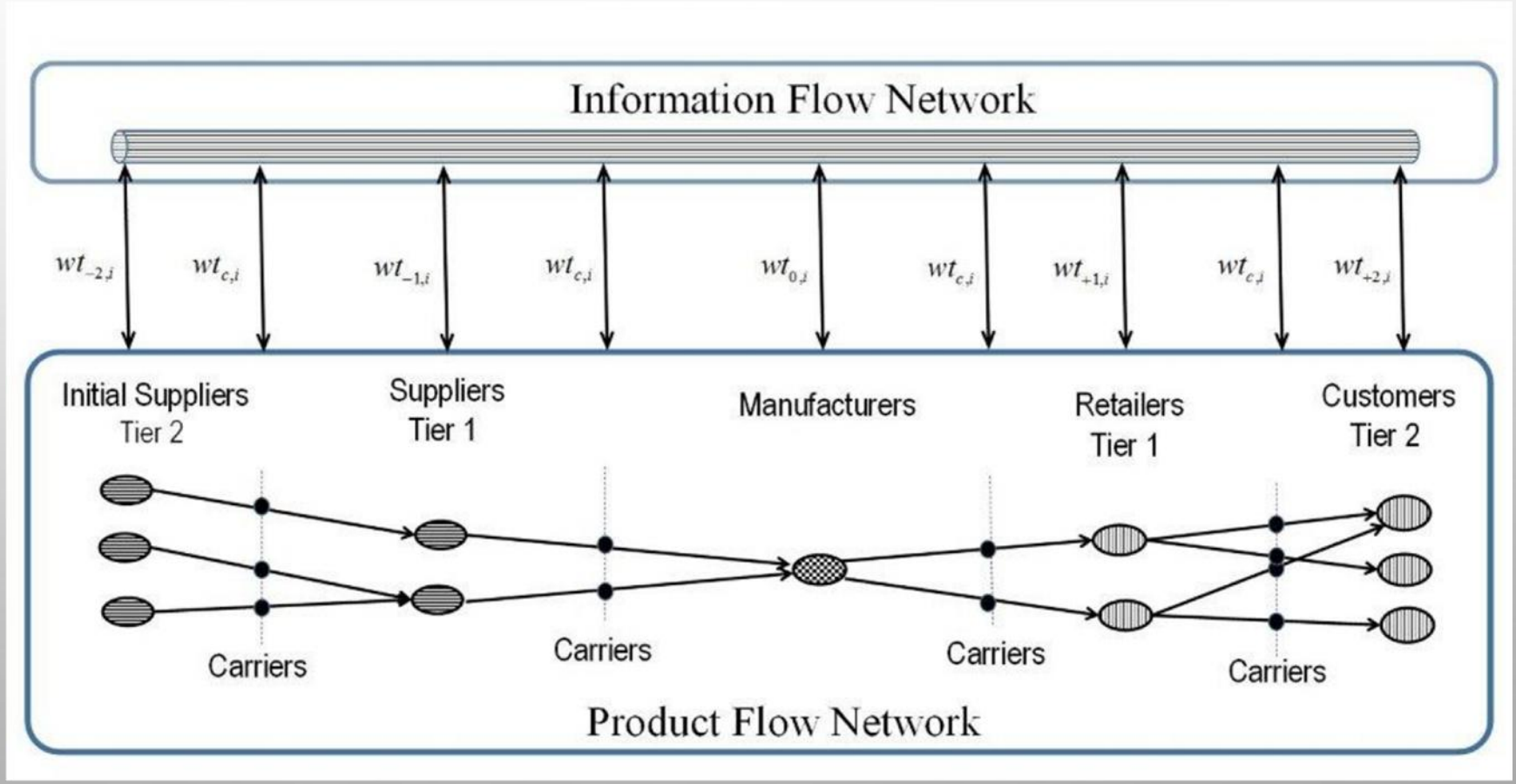
Goals for efficiency

— prioritize efforts to mitigate systematic vulnerabilities

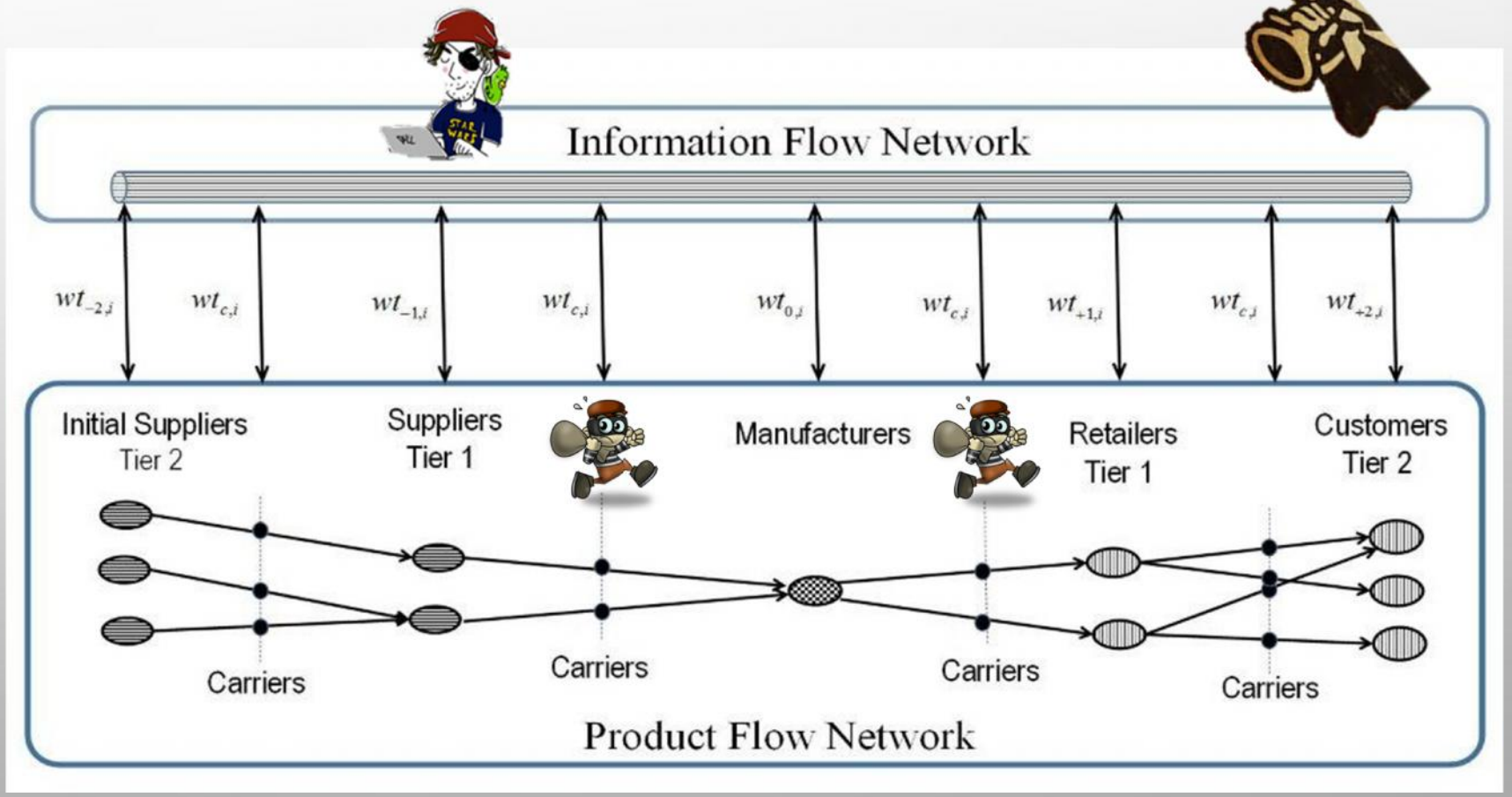
— Plans to reconstitute the flows after disruptions adopted

National Strategy for Global Supply Chain Security

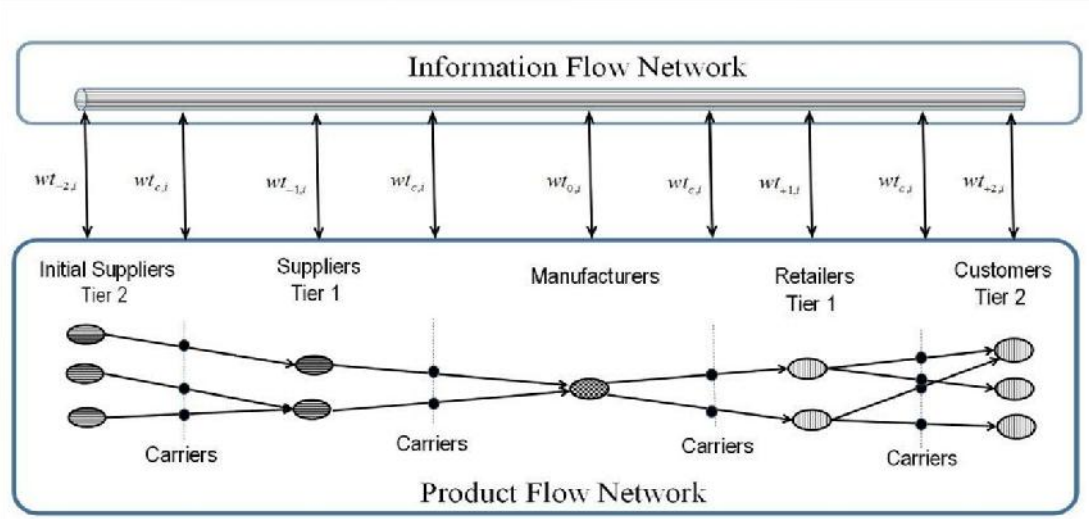
Introduction- Model



Introduction- Adversarial Model



Introduction- Adversarial Model



Adversaries

— Insiders (misbehaviour)

— Outsiders (hackers)

Attacks

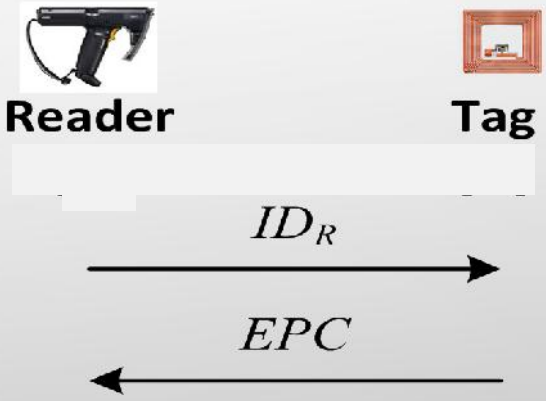
— Privacy (Tracking competitor goods)

— Integrity (thefts)

— Availability (detain/obstruct a shipment)

Introduction- RFID deployments

Basic



UHF tags

— Range: 20 feet/6 meters

— Power constrained devices

Cryptographic primitives

— Lightweight (basic level)

— Symmetric (medium level)

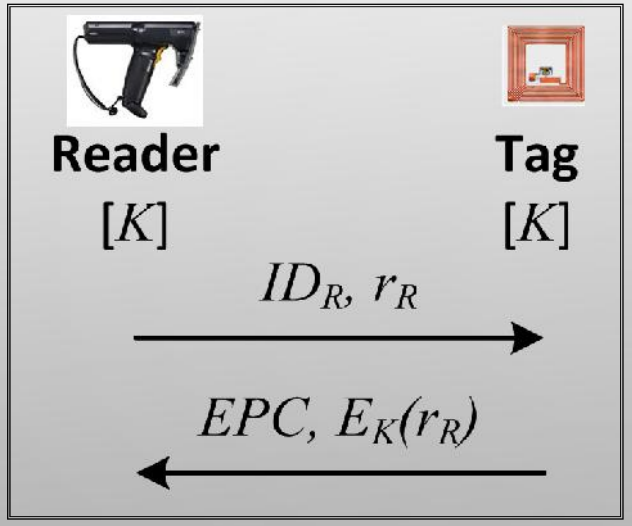
— Asymmetric (high level)

Introduction- RFID deployments, authentication

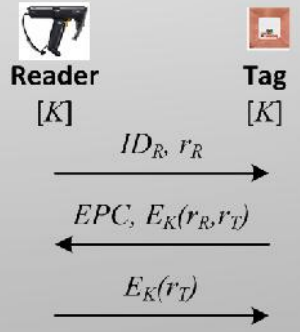
Cryptographic primitives

- Lightweight (basic level)
- **Symmetric (medium level)**
- Asymmetric (high level)

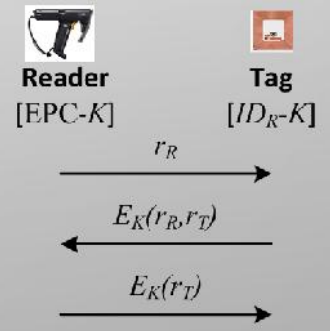
Tag authentication



Mutual authentication



Mutual authentication +Privacy



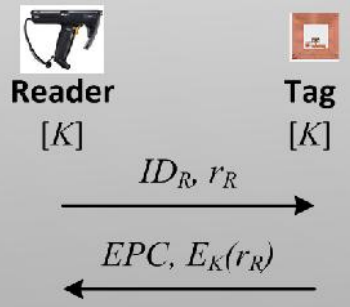
Introduction- RFID deployments, authentication

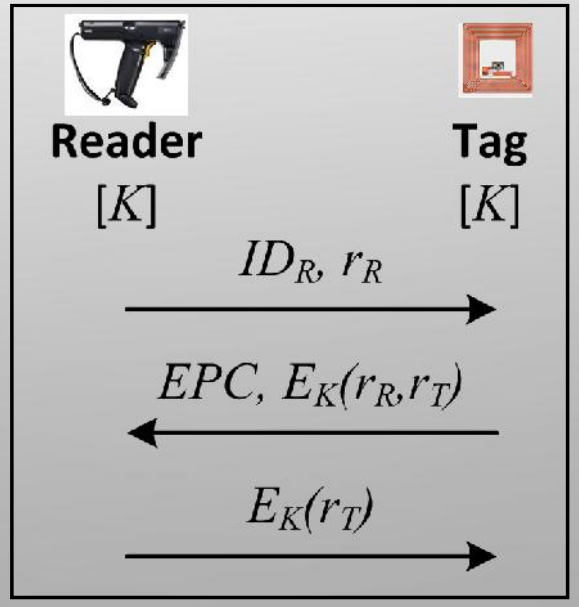
Cryptographic primitives

- Lightweight (basic level)
- **Symmetric (medium level)**
- Asymmetric (high level)

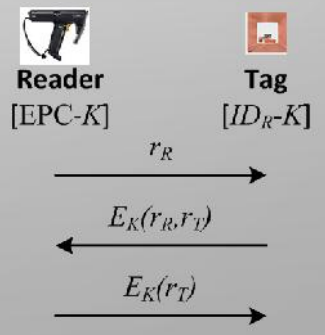
Mutual authentication

Tag authentication





Mutual authentication +Privacy



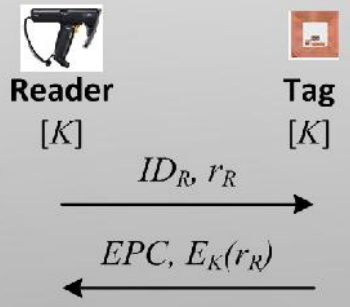
Introduction- RFID deployments, authentication

Cryptographic primitives

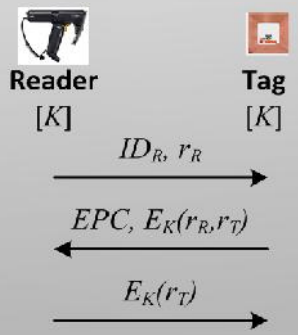
- Lightweight (basic level)
- **Symmetric (medium level)**
- Asymmetric (high level)

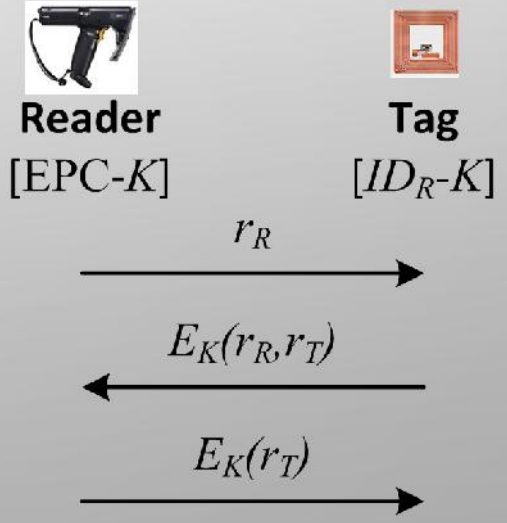
Mutual authentication +Privacy

Tag authentication

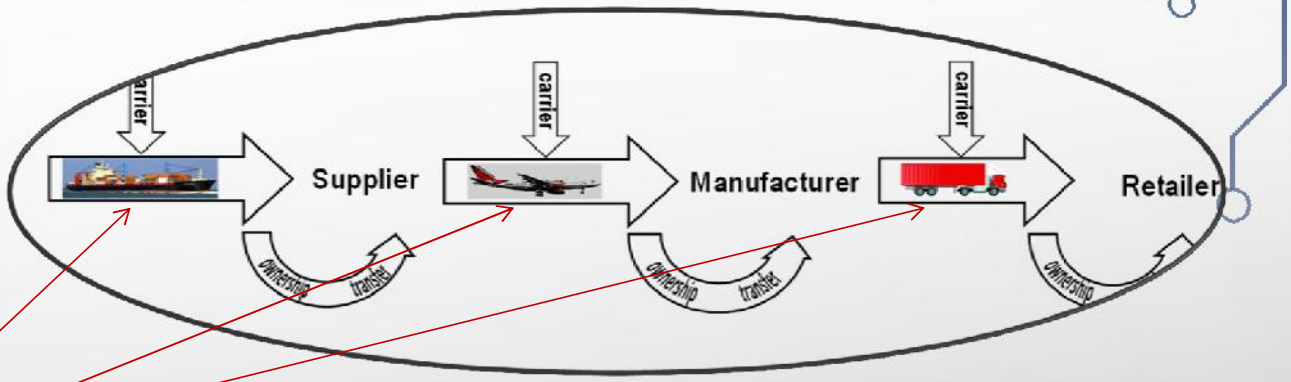


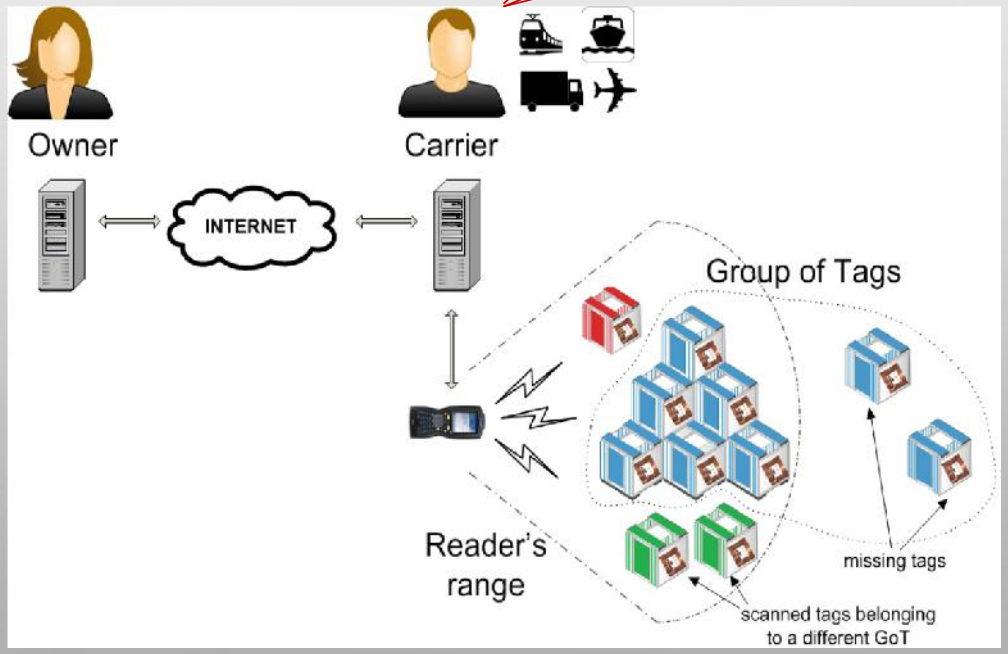
Mutual authentication





Shipping Flow Links

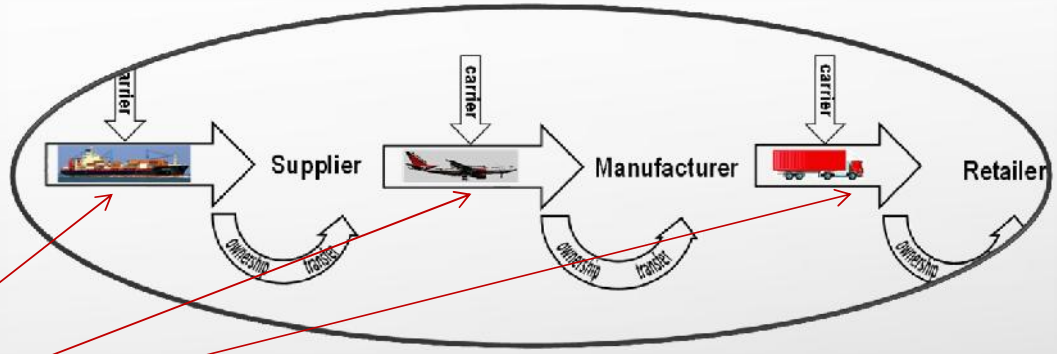


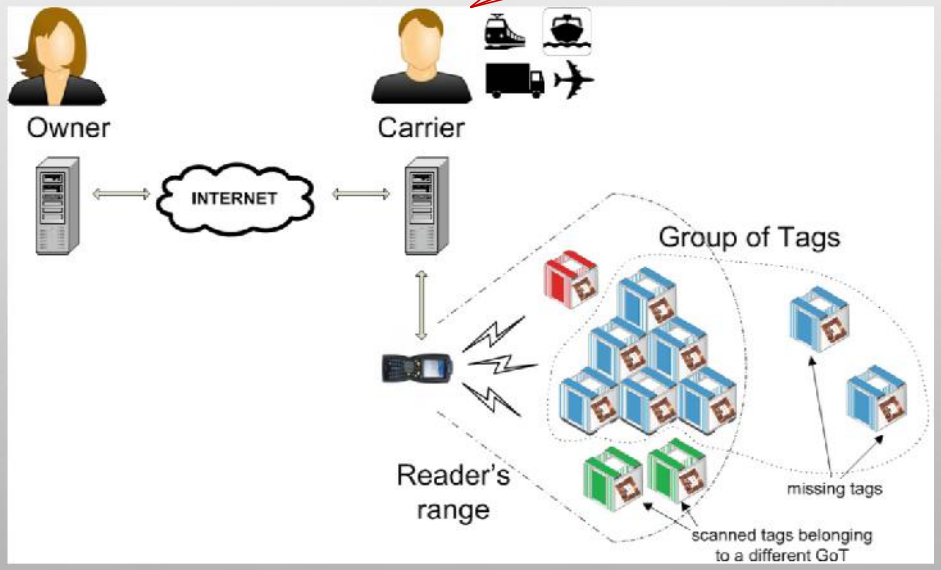


Ideal case

— No missing tags
— Carrier Trusted
— Full connectivity → Owner can communicate with tags directly

Shipping Flow Links



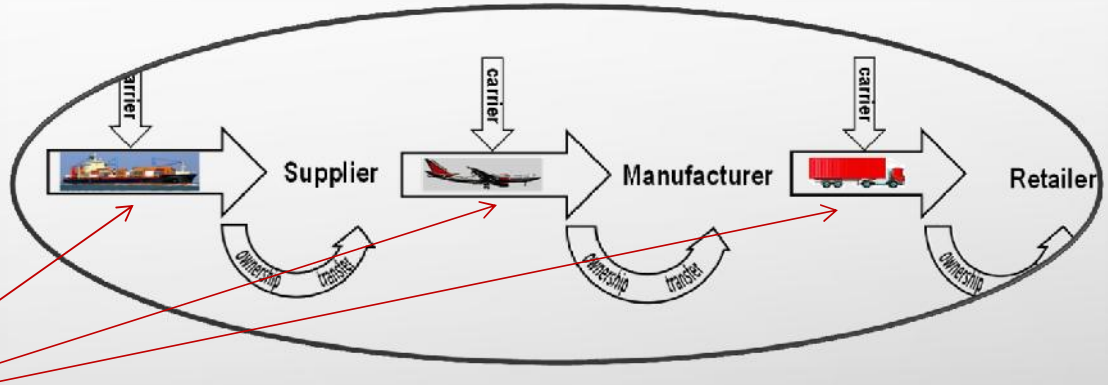


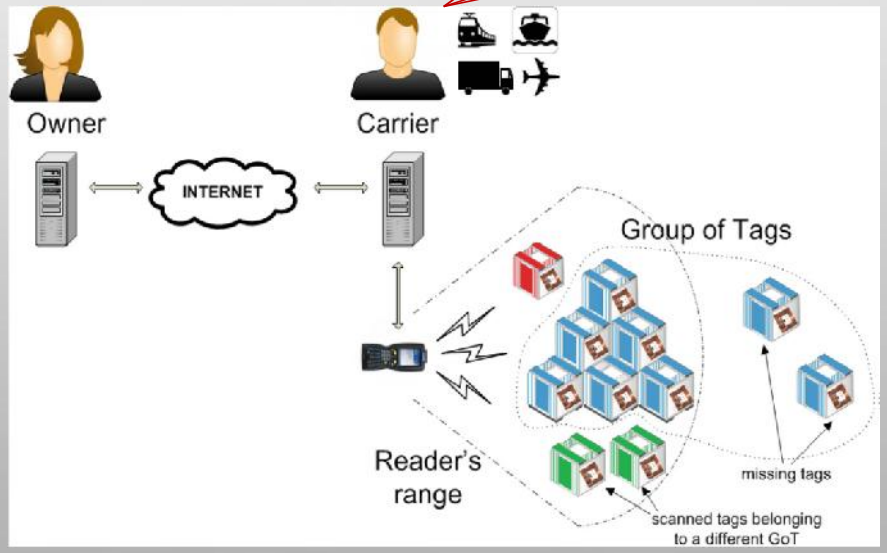
Ideal case

- No missing tags
- Carrier Trusted
- Full connectivity → Owner can communicate with tags directly

And when this does not happen?

Shipping Flow Links

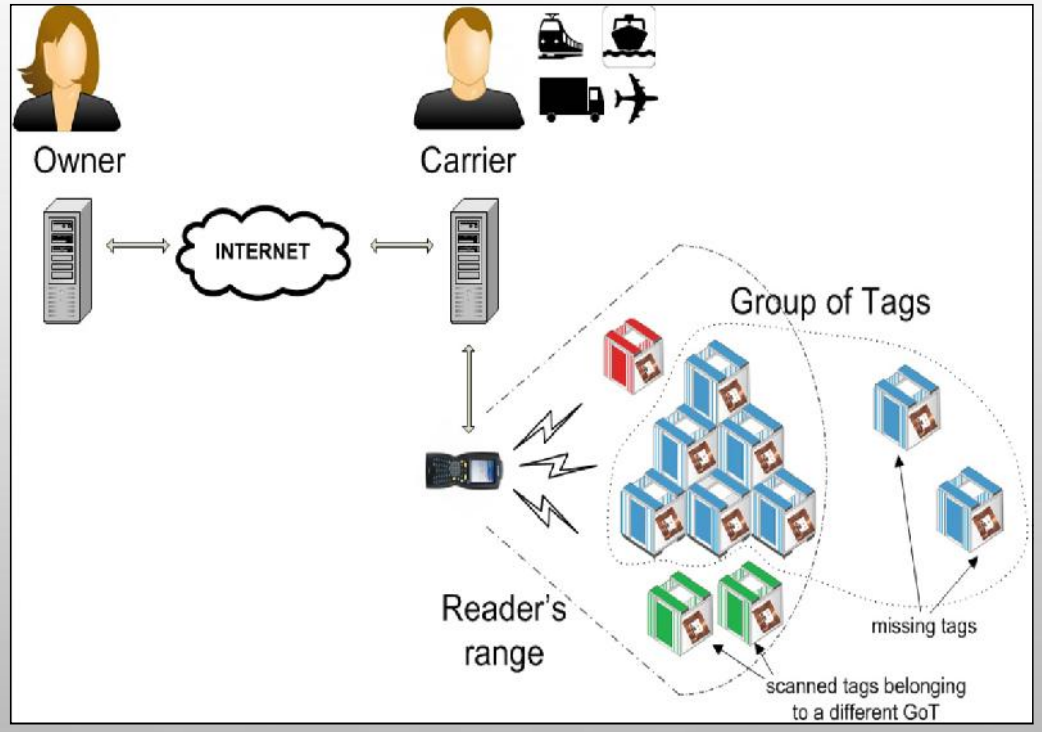




Practical case

— There are missing tags
— Carrier is not Trusted
— Batch connectivity

Shipping Link-missing tags



Goals with Missing Tags

— Detect the event
— Estimate the number
— Identify the missing tags

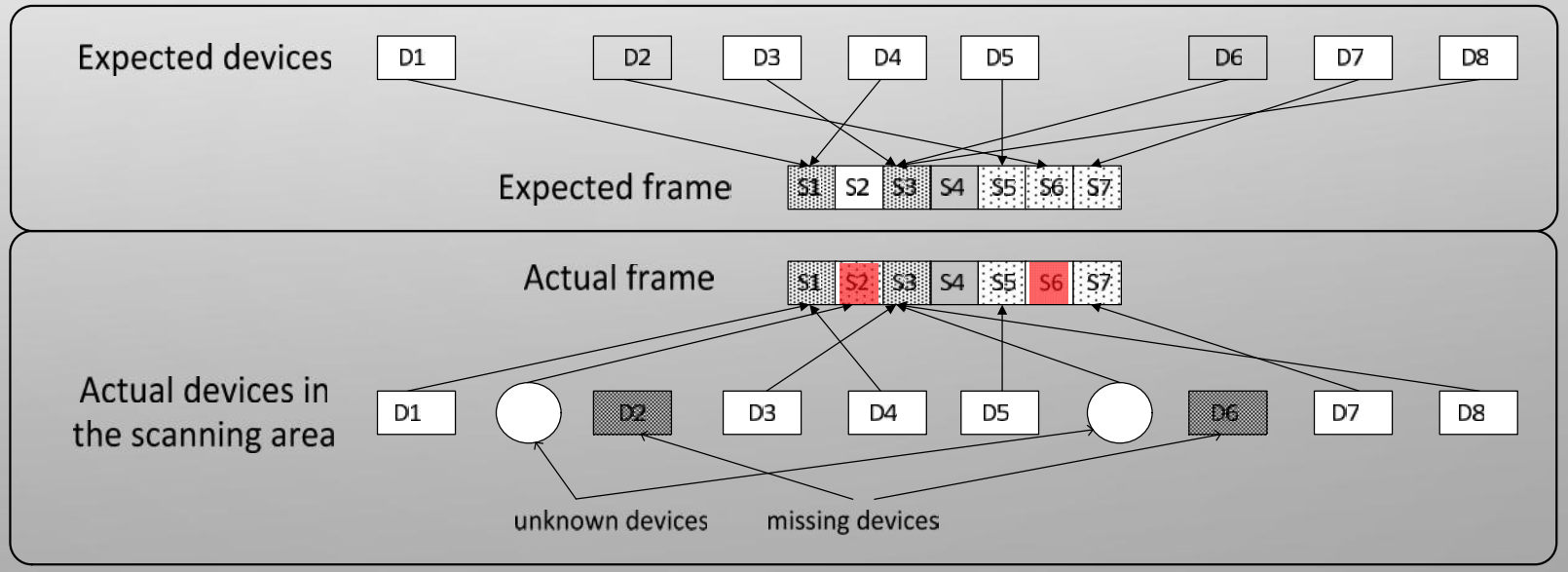
1. with packing list

2. without packing list

Shipping Link-missing tags, with packing list

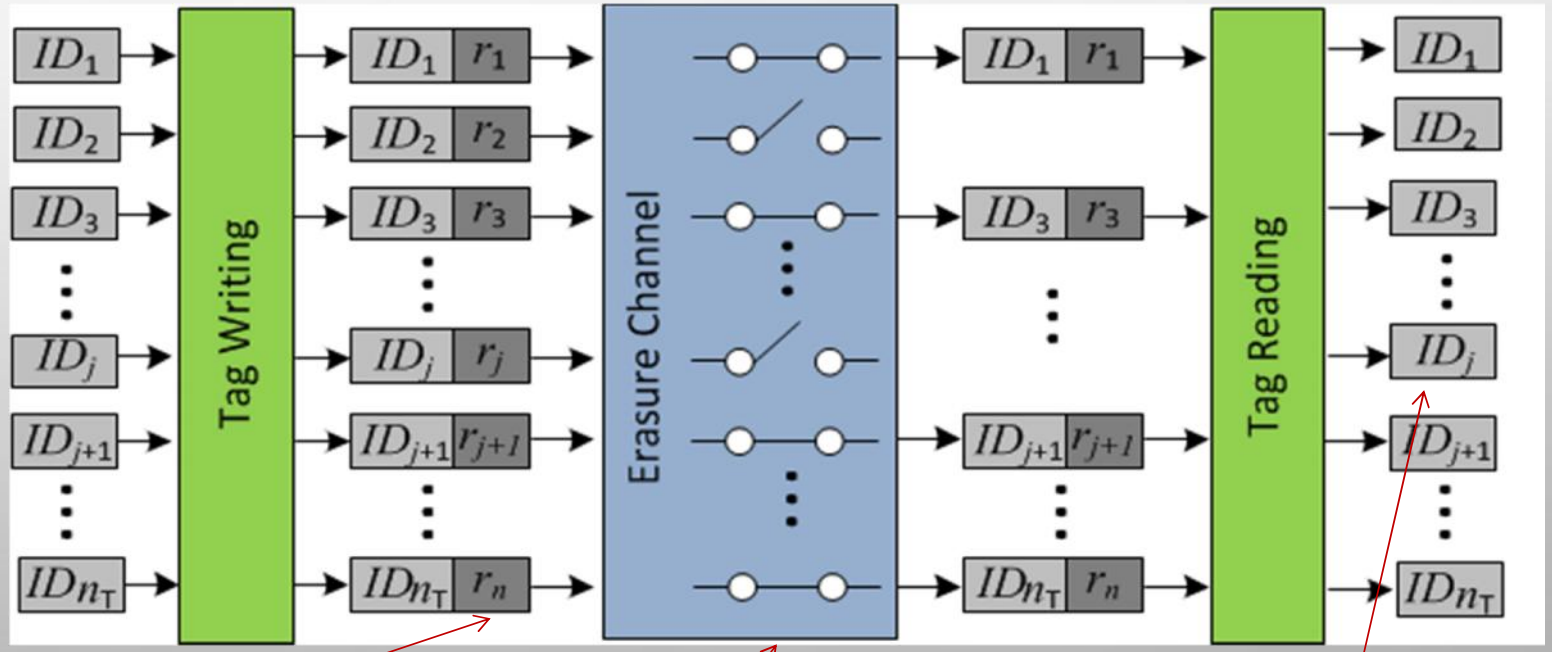
—Sequential process is inefficient → detect the event and the number with certain probability and accuracy respectively.

—Two options: tree-based and **Aloha based** protocols. For the later, the reader sends the size of the frame *f* and a number *R*, and tags compute the slot as *hash* (*R*, *ID*) mod *f* .



Shipping Link-missing tags, without packing list

Grouping codes (Forward Error Correction codes) are used

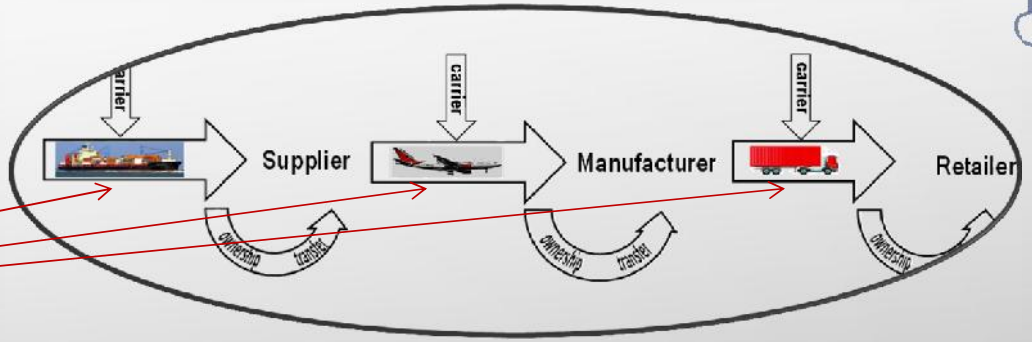


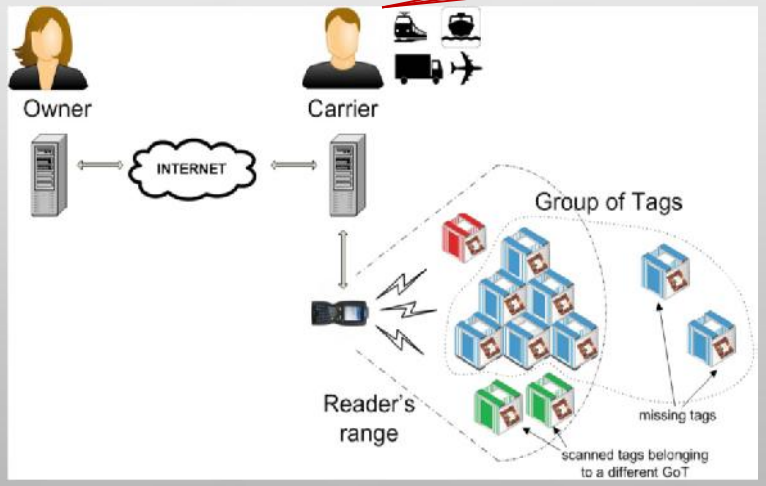
Some redundancy is stored

Erasure Channel: output is identical to the input or nothing

Redundancy of the remaining tags is used to recover the identities of missing tags

Shipping Link- Integrity Proof, without packing list





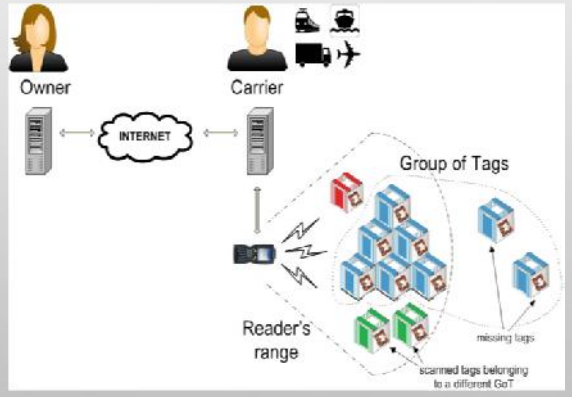
Practical case

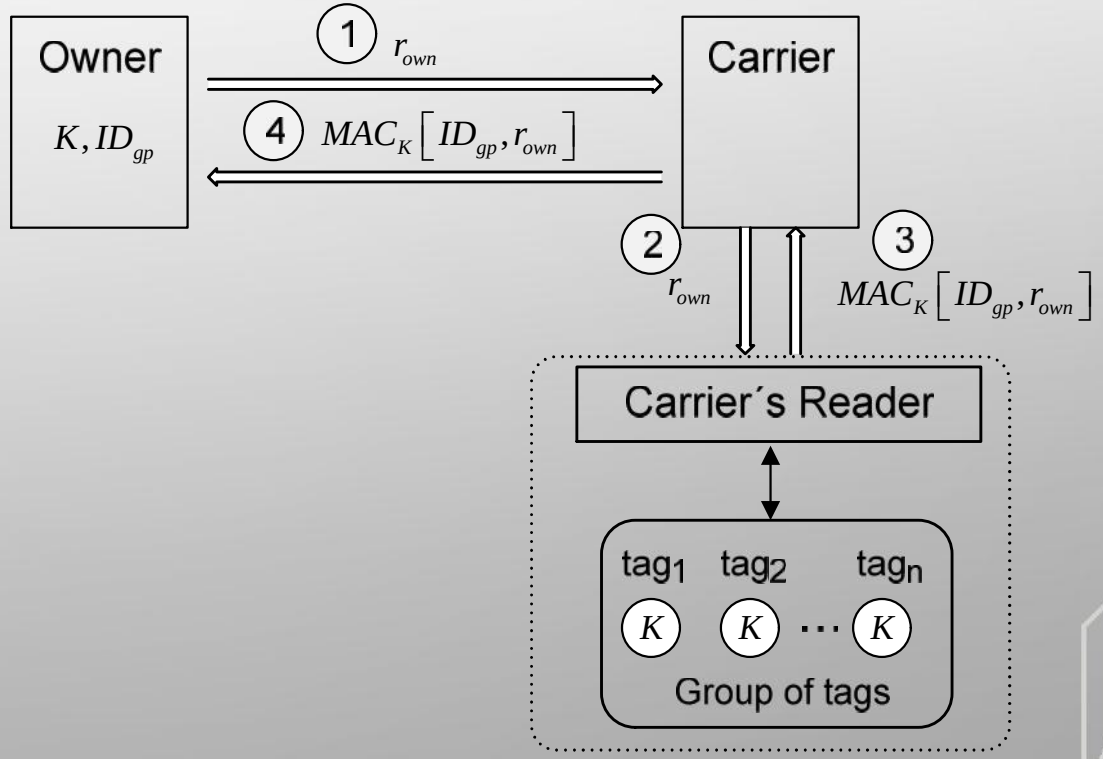
— There are missing tags
— Carrier is not Trusted
— Batch connectivity

Grouping proofs (integrity proofs)

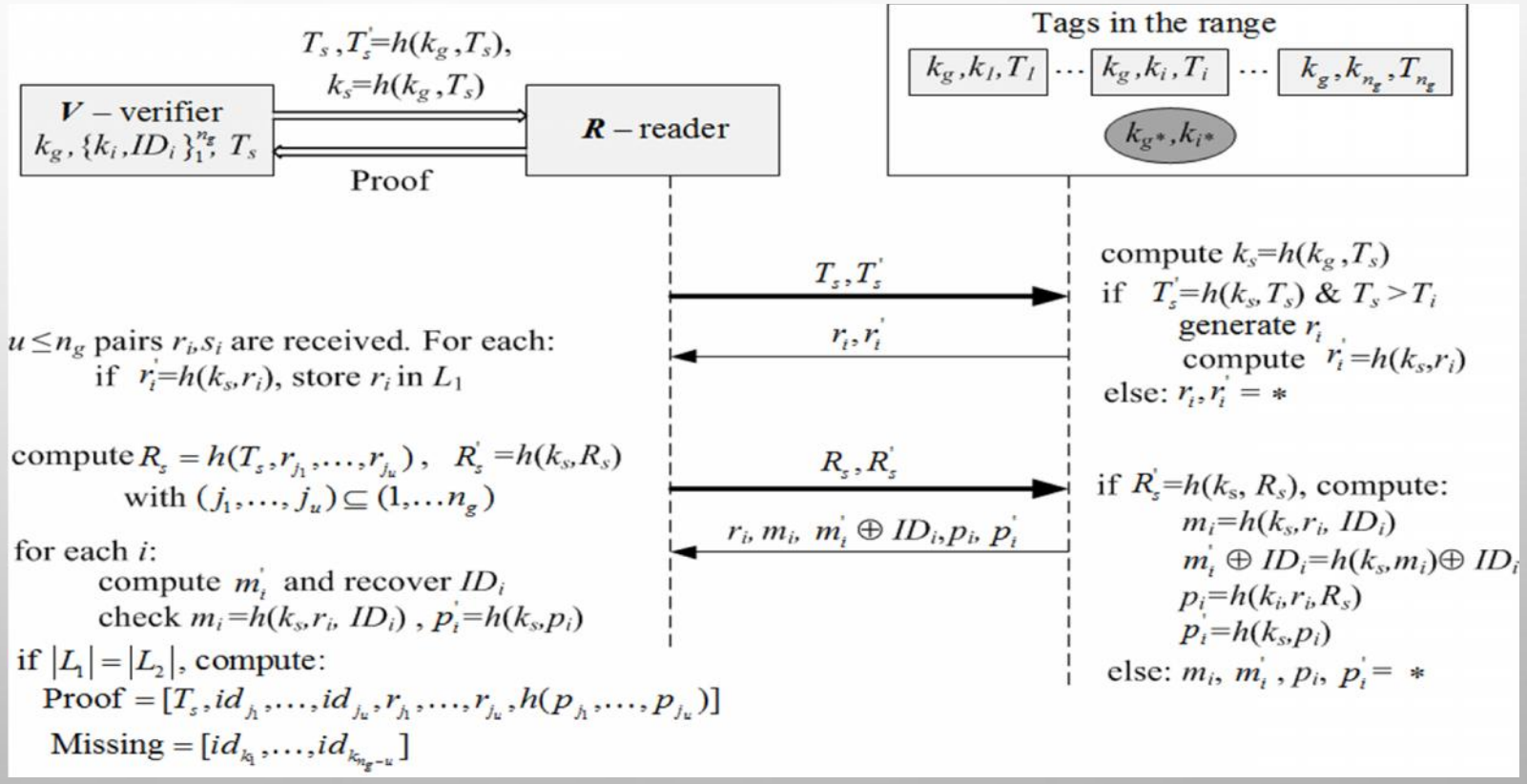
Shipping Link- Integrity Proof, without packing list

– **Symmetric Key Cryptography is assumed**



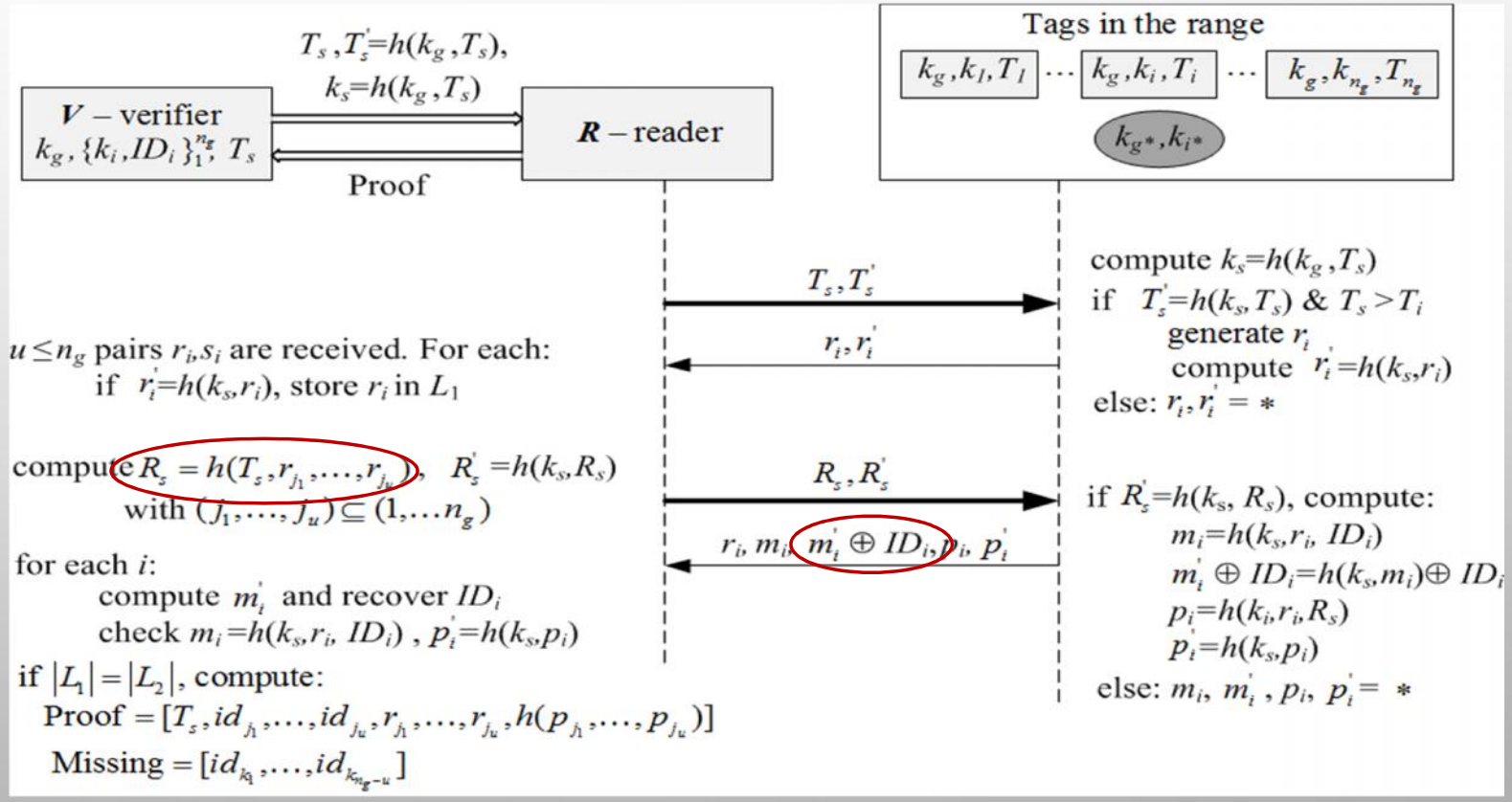


Shipping Link- Integrity Proof, without a packing list



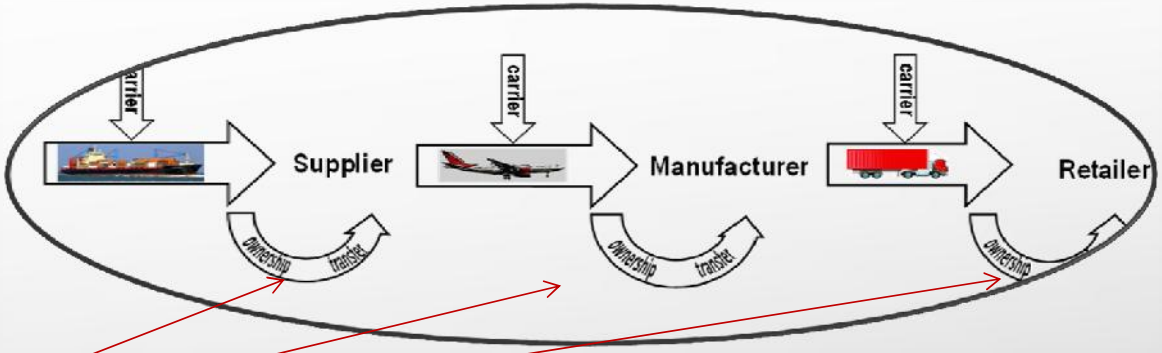
Two-rounds anonymous grouping proof with missing tag identification

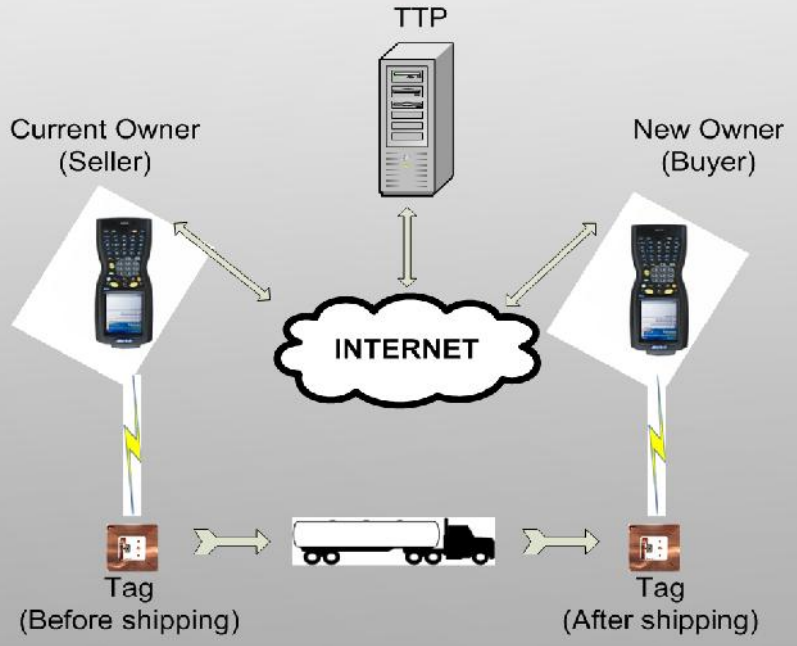
Shipping Link- Integrity Proof, without a packing list



Two-rounds anonymous grouping proof with missing tag identification

Ownership Transfer





Ownership Transfer

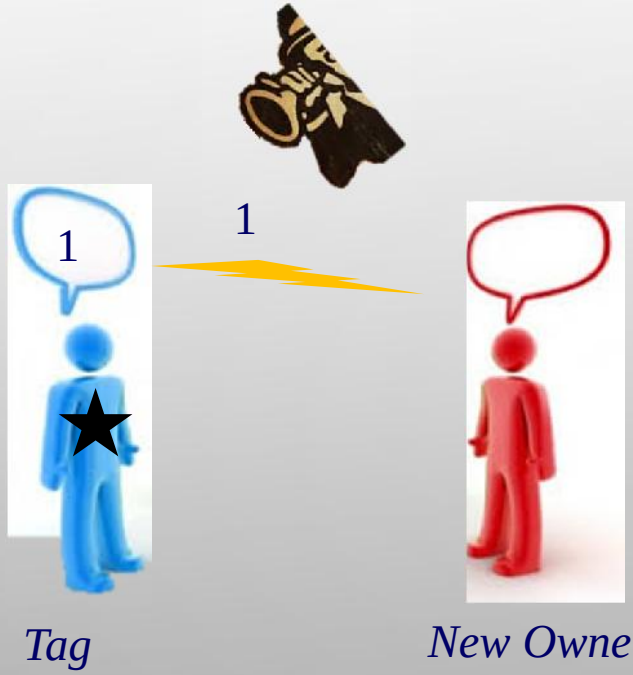
— Secure

— Guarantee the privacy of both parties

Current owner cannot trace the tag once ownership is transferred. This is challenging because the new owner does not share any *private information* with the tag that the previous owner does not know.

Ownership Transfer

Current owner-eavesdropper



New owner and tag cannot agree a new *private* key because the current owner is eavesdropping

Options to guarantee the privacy

— TTP → not appropriate for decentralized process

— Isolated Environments → weak threat model

Ownership Transfer

Options to guarantee the privacy

— TTP → not appropriate for decentralized process

— Isolated Environments → weak threat model

Channels with positive secrecy capacity

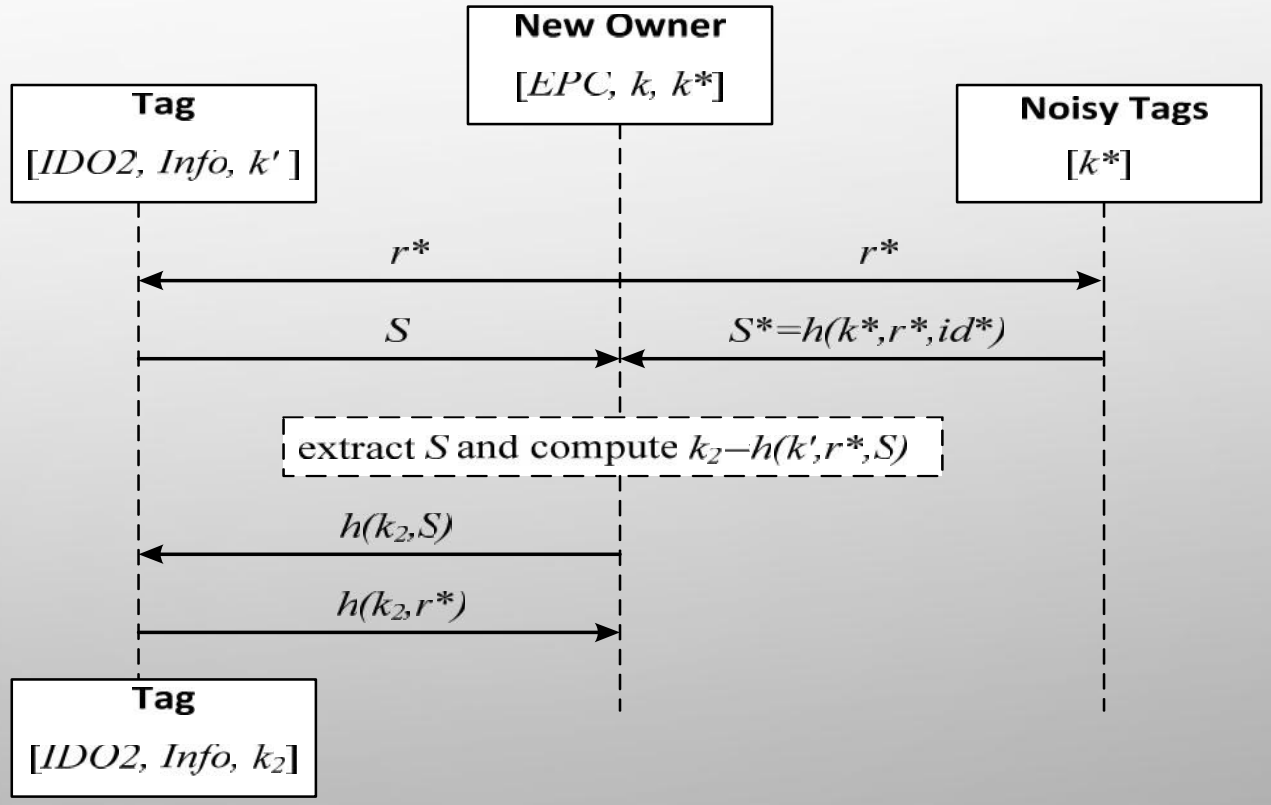
Example

Tag is hidden in the crowd

1101000100

shared secret

Ownership Transfer

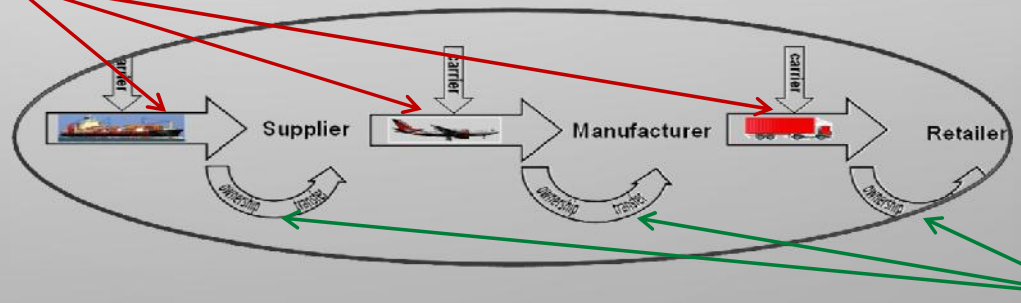


Key Update Protocol that uses noisy tags to guarantee the privacy of the new owner

Conclusions

1. Security and resilience in the supply chain will become even more important in the future.
2. Threats come from different actors (insiders and outsiders)
3. The security of the different segments of the supply chain must be guaranteed:

…by using grouping proofs and missing tag detection mechanisms for the transit flows



…and ownership transfer with positive secrecy capacity

Any Questions