5G Architecture Overview and Security

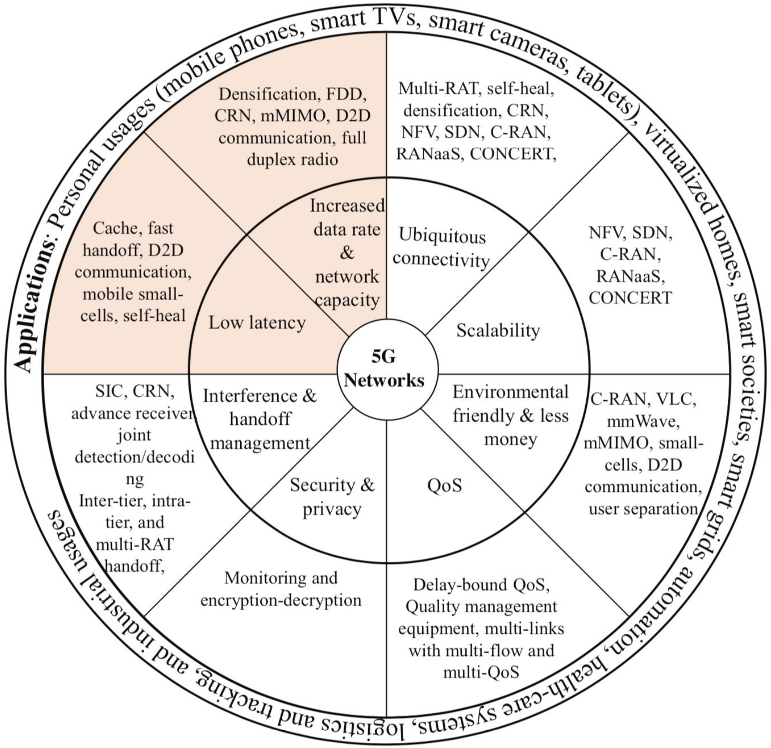
Wireless Systems and Networks

A cura di Simone Bonfante

Introduction

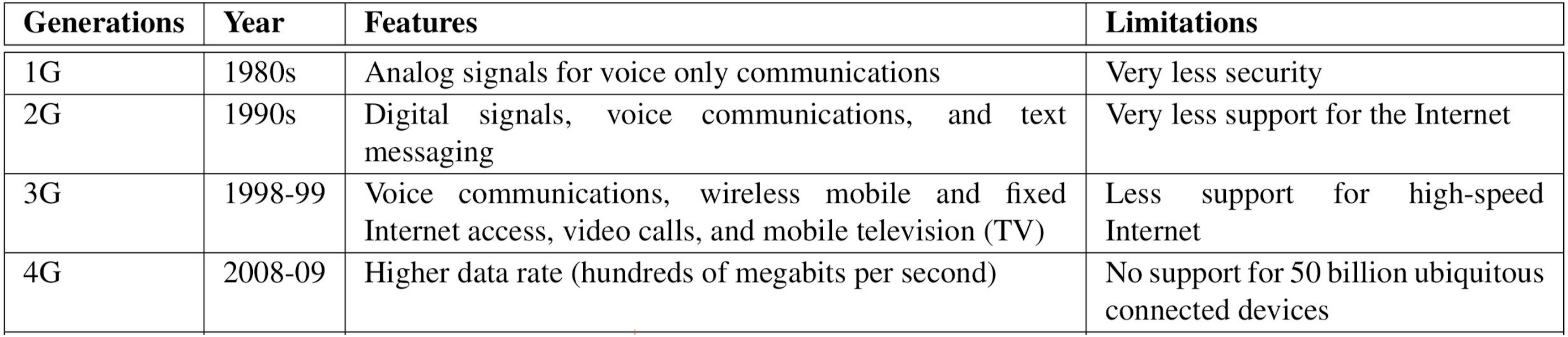
- The increase of 3D: **D**evice, **D**ata, **D**ata transfer rate
- Features:
  - Ubiquitous connectivity
  - Zero latency
  - High-speed Gigabit connection

Requirements, Technologies and Applications



5G Networks
Increased data rate & network capacity
Ubiquitous connectivity
Scalability
Environmental friendly & less money
QoS
Security & privacy
Interference & handoff management
Low latency
Densification, FDD, CRN, mMIMO, D2D communication, full duplex radio
Multi-RAT, self-heal, densification, CRN, NFV, SDN, C-RAN, RANaaS, CONCERT,
NFV, SDN, C-RAN, RANaaS, CONCERT
C-RAN, VLC, mmWave, mMIMO, small-cells, D2D communication, user separation
Delay-bound QoS, Quality management equipment, multi-links with multi-flow and multi-QoS
Monitoring and encryption-decryption
SIC, CRN, advance receiver joint detection/decodi ng Inter-tier, intra-tier, and multi-RAT handoff,
Cache, fast handoff, D2D communication, mobile small-cells, self-heal
Applications: Personal usages (mobile phones, smart TVs, smart cameras, tablets), virtualized homes, smart societies, smart grids, automation, health-care systems, logistics and tracking, and industrial usages

From 1G to 4G



Generations	Year	Features	Limitations
1G	1980s	Analog signals for voice only communications	Very less security
2G	1990s	Digital signals, voice communications, and text messaging	Very less support for the Internet
3G	1998-99	Voice communications, wireless mobile and fixed Internet access, video calls, and mobile television (TV)	Less support for high-speed Internet
4G	2008-09	Higher data rate (hundreds of megabits per second)	No support for 50 billion ubiquitous connected devices

Security issues in 4G

- **Wi-Max:**
  - DoS attacks
  - DDoS attacks
  - Replay attacks
  - Eavesdropping

- **LTE:**
  - Faulty geographical location tracking
  - Authentication
  - DoS attacks and data modification
  - Scrambling attacks

Why 4G isn't enough?

- No support for bursty data traffic
- Inefficient utilization of processing capabilities of a base-station
- Co-channel interference
- No support for heterogeneous wireless networks
- No separation of indoor and outdoor users

Desideratum of 5G Networks

- Dramatic upsurge in device scalability
- Massive data streaming and high data rate
- Spectrum utilization
- Ubiquitous connectivity
- Zero latency

Two-tier Architecture

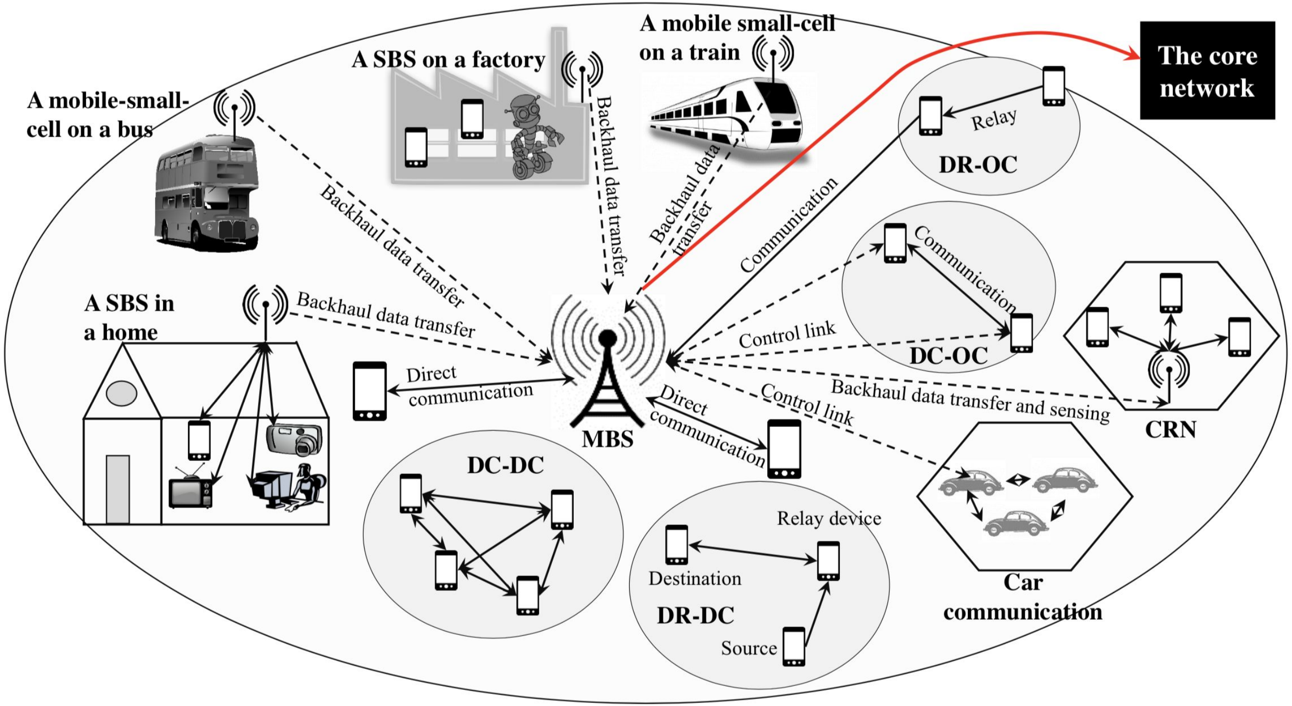
Advantages

- High data rate and efficient spectrum use
- Energy and Money saving
- Less congestion to a MBS
- Easy handoff

Disadvantages and issues

- Cost and operational reliability
- Frequent authentication
- Interference management
- Backhaul data transfer

5G Multi-tier Architecture



Massive MIMO

Most wireless users stay **inside** for about **80%** of the time and **outside** for about **20%** of the time.
The communication between inside and outside improves with the use of mMIMO.
Advantages:

- **Excellent spectral efficiency**, obtained by spatial multiplexing of many terminals in the same time-frequency resource.
- **Excellent energy efficiency**, thanks to the antenna arrays that allow a reduction in radiated power

Specifications

Beamforming

It uses multiple antennas to control the **direction** of the waves by appropriately weighing the **amplitude** and **phase** of the individual signals.

Radiating elements that transmit the same signal at an **identical wavelength and phase** to create a single antenna with a longer and more focused flow

Full Duplex

Radios cellular networks will have to reduce their spectrum needs in half as **only one channel** is used to obtain the same performances.

Separate channels, both for **uplink** and **downlink**

Cognitive Radio Network

A cognitive radio network (CRN) is a collection of cognitive radio nodes (SUs) that **exploit** the existing **spectrum** opportunistically, **remove interference** among cells and **minimizing energy** consumption in the network.

Cognitive technique in SBS

- Cognitive module
- Cognitive engine
- Autoconfiguration module

Device-to-Device Communication

Challenges: Interference, Resource allocation, Delay-sensitive processing.

D2D communication types:

- Device relaying with operator controlled link establishment (**DR-OC**)
- Direct D2D communication with operator controlled link establishment (**DC-OC**)
- Device relaying with device controlled link establishment (**DR-DC**)
- Direct D2D communication with device controlled link establishment (**DC-DC**)

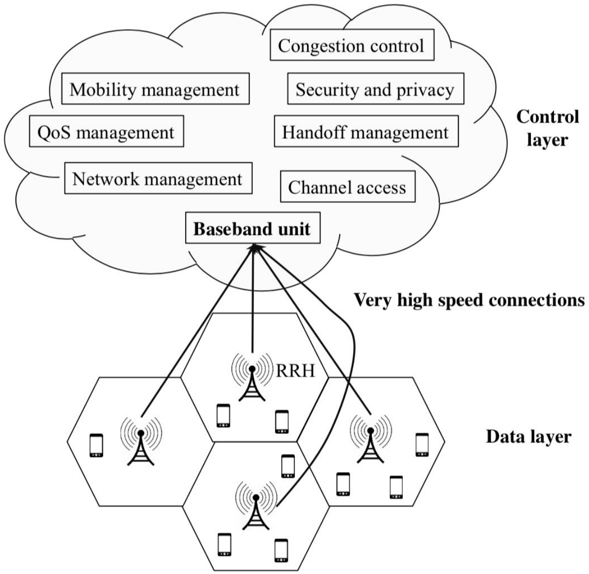
Cloud-based radio access network

Two C-RAN possible models

- *Full-centralized* C-RAN
- *Partially-centralized* C-RAN

Two layers:

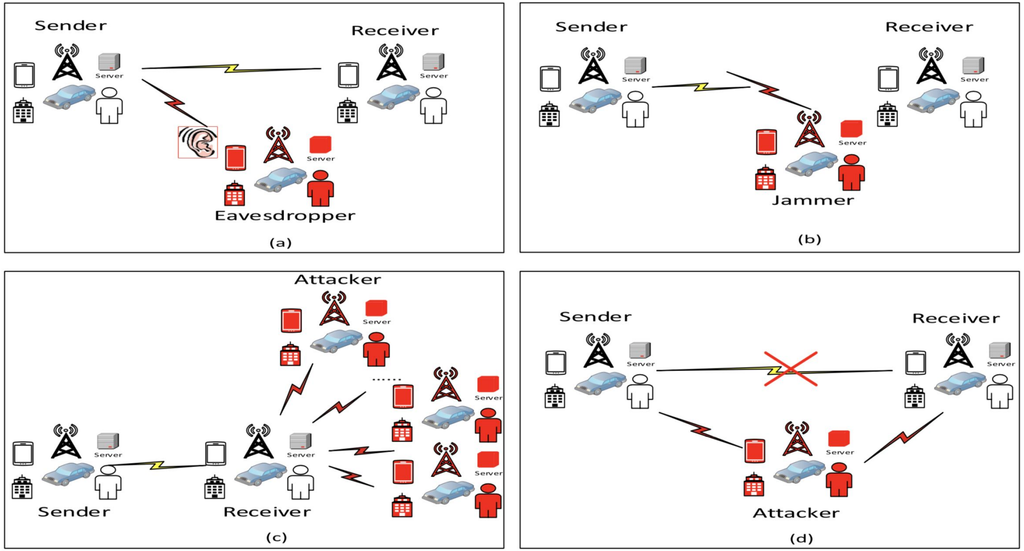
- *Data layer* which contains physical resources
- *Control layer* which performs resource management



5G Security

Two main approaches:

- **Cryptographic**
    - secret key
    - public key
- **P**hysical **L**ayer **S**ecurity secret key through public channel



Security Services 1/2

- Authentication
    - message auth
    - entity auth

5G requires authentication not only between **UE**s but also between other **third parties** such as service providers

- Confidentiality
    - data confidentiality
    - privacy

Shared **private key**
PLS can support confidentiality service against jamming and eavesdropping attacks

Security Services 2/2

- Availability

Degree to which a service is accessible.

DSSS and **FHSS** are two classical PLS solutions

- Integrity

Integrity prevents information from being **modified** or **altered** by active attacks from **unauthorized** entities

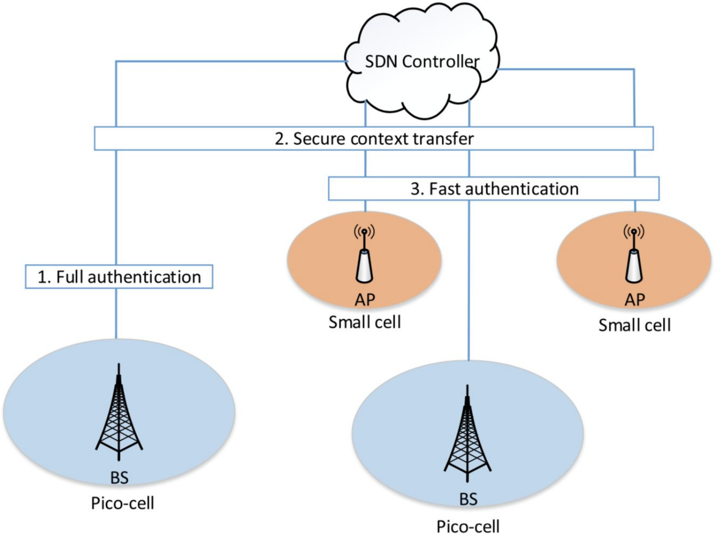
Mutual authentication can provide integrity service.

Possible Solutions - Authentication 1/2

SDN

Secure-context-information (SCI) transfer based on the user-inherent physical layer attributes.

a) Full authentication in one cell.
b) Applied in other cells with **MAC address verification.**



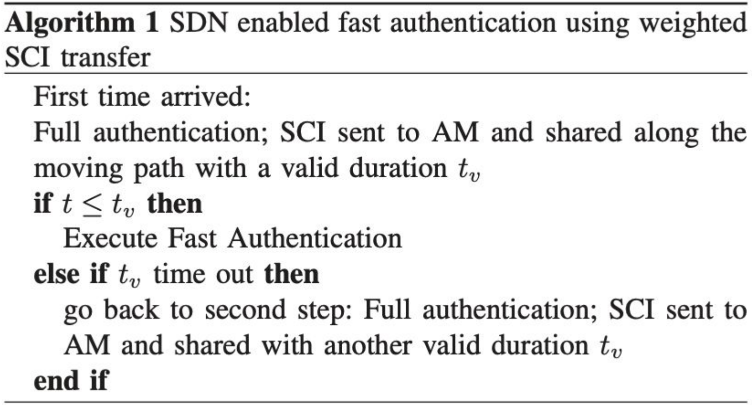
Possible Solutions - Authentication 1/2

SDN

One physical layer attribute **is not** considered a reliable solution.

3 **types** of fingerprints for mobile UEs:

- Software-based
- Hardware-based
- Channel / location-based



Algorithm 1 SDN enabled fast authentication using weighted SCI transfer

```
First time arrived:
Full authentication; SCI sent to AM and shared along the moving path with a valid duration $t_v$
**if** $t \leq t_v$ **then**
    Execute Fast Authentication
**else if** $t_v$ time out **then**
    go back to second step: Full authentication; SCI sent to AM and shared with another valid duration $t_v$
**end if**
```

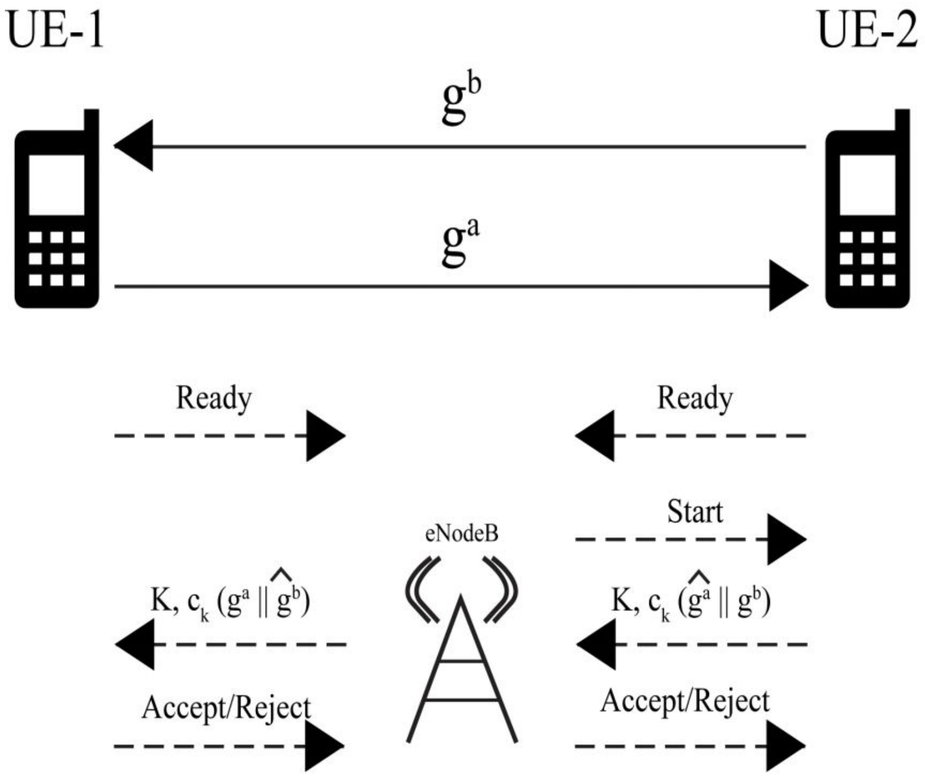
Possible Solutions - Authentication 2/2

Cyclic Redundancy Check

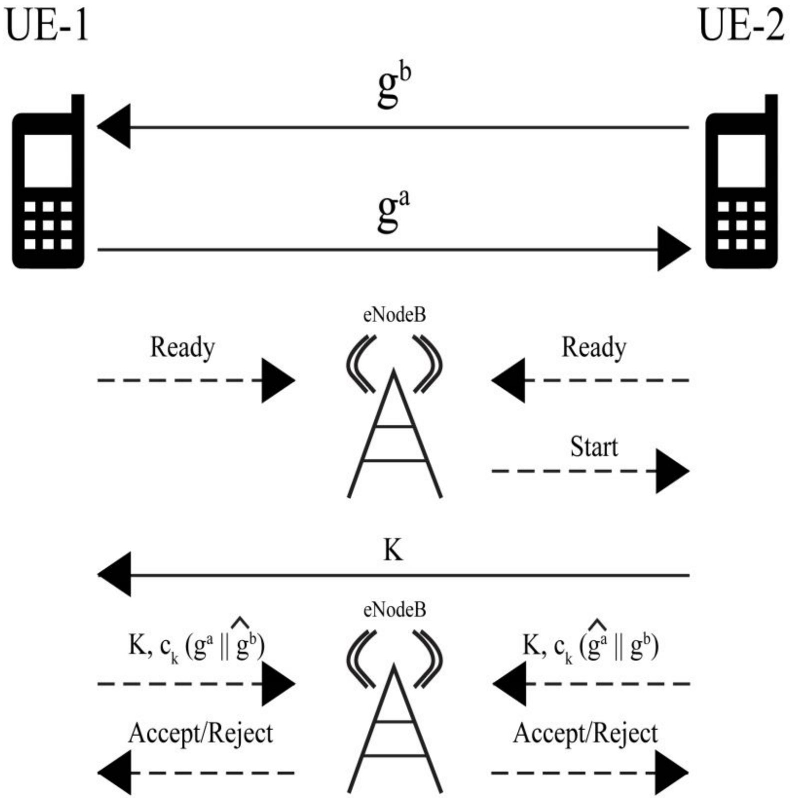
(CRC)-based message authentication which can detect any double-bit errors in a single message.

- The algorithm outputs an auth-tag based on a secret key and the message.
- The adversary doesn't have the particular polynomial g(x).
- The generator polynomial is changed periodically.

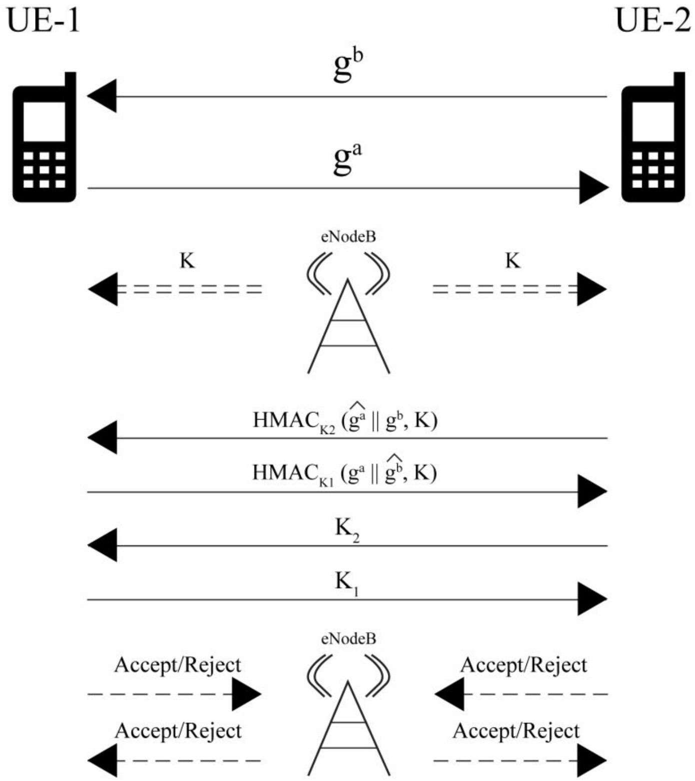
Possible Solutions - Key Management 1/3



Possible Solutions - Key Management 2/3

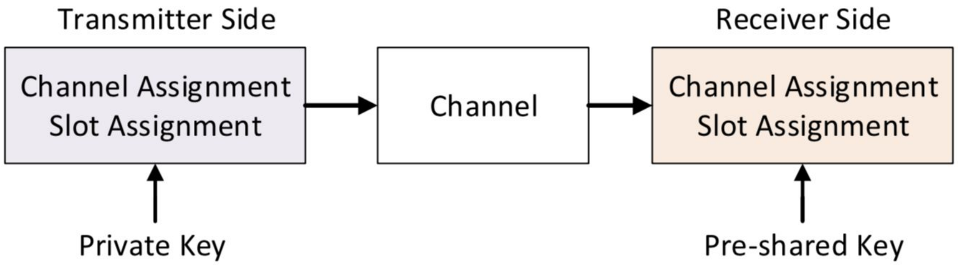


Possible Solutions - Key Management 3/3



Possible Solutions - Availability 1/2

Jamming and DoS typical attacks.
Anti-jamming schemes use the frequency-hopping technique, but don't work efficiently for dynamic spectrum access users.
Pseudorandom time hopping anti-jamming scheme

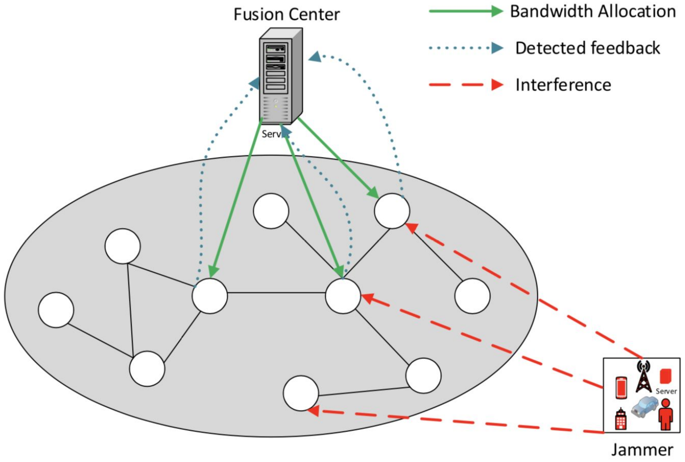


Possible Solutions - Availability 2/2

Nodes with limited computational capabilities

Fusion Center:

- Allocates more bits for reporting the interference
- Instructs the target node to increase its transmit power

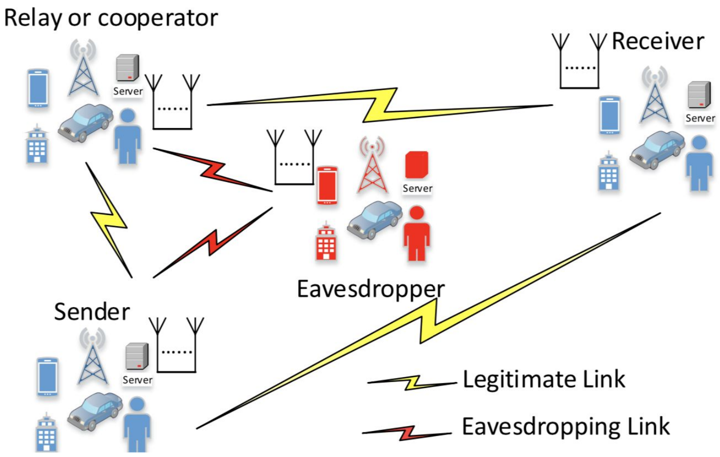


Possible Solutions - Data Confidentiality

Power Control:
It aims to control the transmit power to avoid eavesdropping.
With relay, **Without** relay.

Artificial Noise:
The legitimate receiver generates artificial noise (AN) to impair the intruder’s channel

Signal Processing:
Original symbol phase rotated (OSPR)



Conclusions

Salient features: zero latency, high speed data transfer and ubiquitous connectivity

Expected **applications and services**:

- Personal usages
- Virtualized homes
- Smart societies
- The tactile Internet
- Healthcare systems
- Industrial usages
- Vehicle-to-Vehicle

Reference

- N. Adem, B. Hamdaoui, and A. Yavuz. Pseudorandom time-hopping anti-jamming technique for mobile cognitive users. In 2015 IEEE Globecom Workshops (GC Wkshps), pages 1–6, Dec 2015.
- G. Arfaoui, P. Bisson, R. Blom, R. Borgaonkar, H. Englund, E. Félix,F. Klaedtke, P. K. Nakarmi, M. Näslund, P. O'Hanlon, J. Papay, J. Suomalainen, M. Surridge, J. Wary, and A. Zahariev. A security architecture for 5g networks.IEEE Access, 6:22466–22479, 2018.
- D. Fang, Y. Qian, and R. Q. Hu. Security for 5g mobile wireless net-works.IEEE Access, 6:4850–4874, 2018.
- China Mobile Research Institute. C-ran: The road towards green ran. In white paper, Sep. 2011.
- F. Liu, J. Peng, and M. Zuo. Toward a secure access to 5g network. In2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (Trust-Com/BigDataSE), pages 1121–1128, Aug 2018.

Reference

- J. Liu, T. Zhao, S. Zhou, Y. Cheng, and Z. Niu. Concert: a cloud-based architecture for next-generation cellular systems.IEEE Wireless Communications, 21(6):14–22, December 2014.
- V. S. Pandi and J. L. Priya. A survey on 5g mobile technology. In 2017 IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI), pages 1656–1659, Sep. 2017.
- Nisha Panwar, Shantanu Sharma, and Awadhesh Singh. A survey on5g: The next generation of mobile communication.Physical Communication, 01 2016.
- R. Sedidi and A. Kumar. Key exchange protocols for secure device-to-device (d2d) communication in 5g. In2016 Wireless Days (WD), pages 1–6, March 2016.
- S. Vij and A. Jain. 5g: Evolution of a secure mobile technology. In20163rd International Conference on Computing for Sustainable Global Development (INDIACom), pages 2192–2196, March 2016.