KICS
한국통신학회

A Study on Vulnerability of D2D Communication for Cluster-based Service in Cellular Networks

Manya Venissa Adzo Sedem, Taehoon Kim, Jong-Hyun Kim*, Inkyu Bang

Hanbat National University

*Electronics and Telecommunications Research Institute (ETRI)

HANBAT NATIONAL UNIVERSITY

24th June 2022 @ KICS’22

Contents

- Introduction
- Threat Model
- Forged CSI Attack
- Numerical Results
- Conclusion

Introduction

- **D2D Communication**

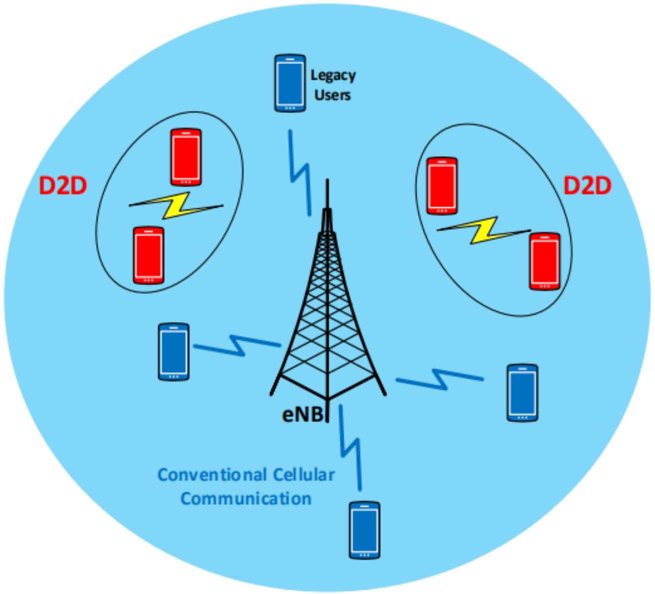
  ❑ Devices in close proximity exchange data directly without going through the core network.

  ❑ Cellular D2D communication promises:

    ✓ ultra-low latency

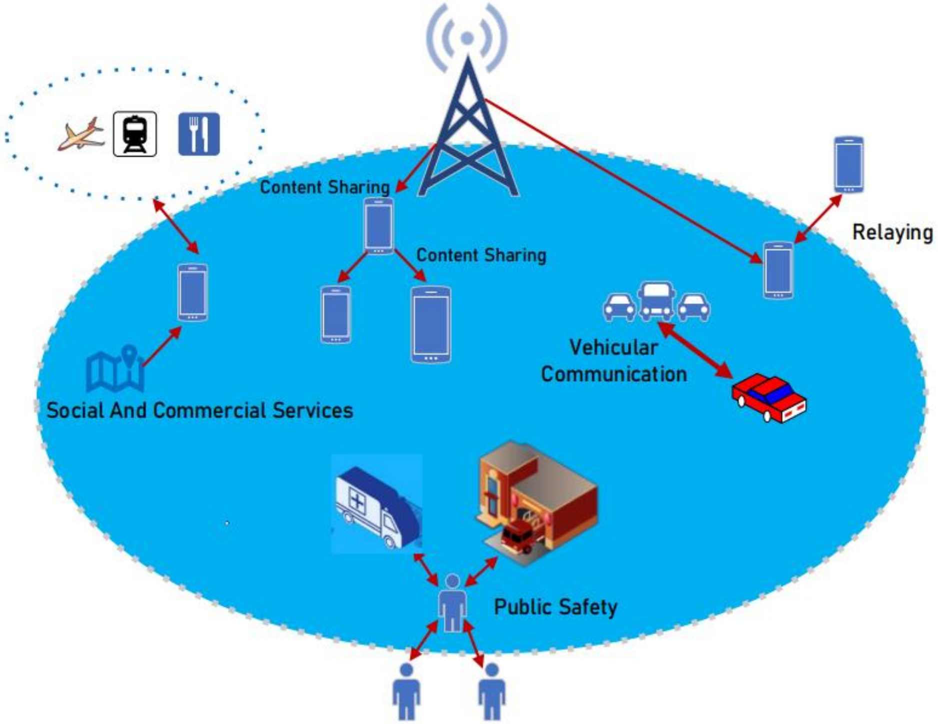
    ✓ flexibility in offloading traffic from the core network

    ✓ increase in spectral efficiency



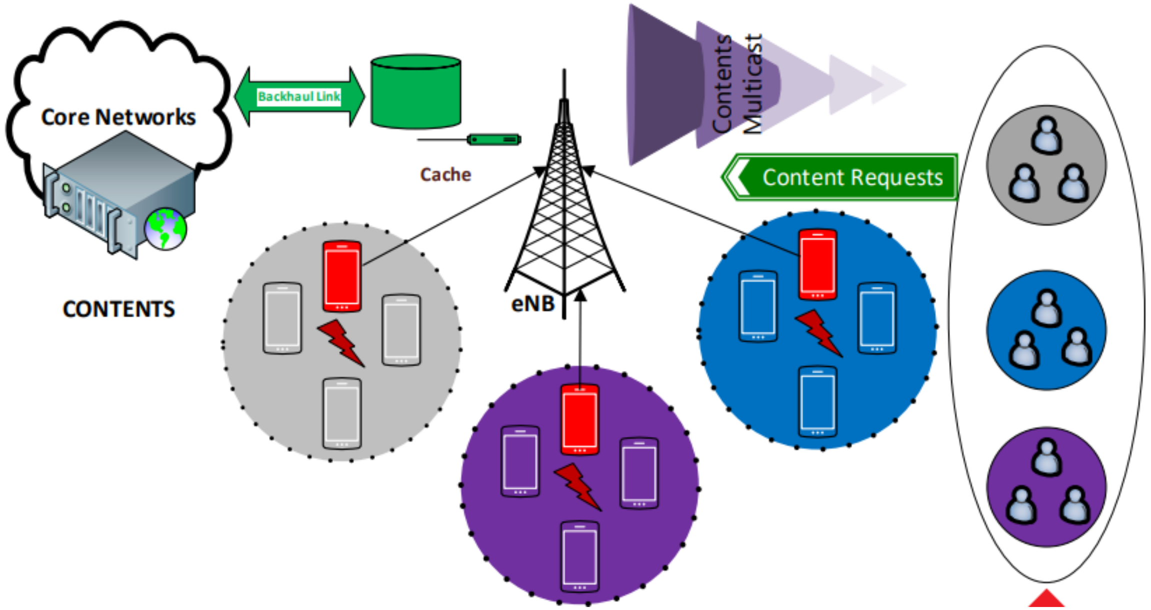
Introduction

- **Applications of D2D Communication**
  - ❑ Local data services
    - ✓Content sharing
      - ○ Higher data rates
      - ○ Lower energy
      - ○ Better power consumption
    - ✓Data and computation offloading
  - ❑ Coverage extension
  - ❑ M2M communication



Introduction

- **D2D Clustering**
  - ❑ Cluster-based D2D can improve network performance in terms of:
    - ✓ throughput
    - ✓ spectral efficiency
    - ✓ energy consumption



Threat Model (1/2)

- **D2D cluster-based communication in cellular networks**

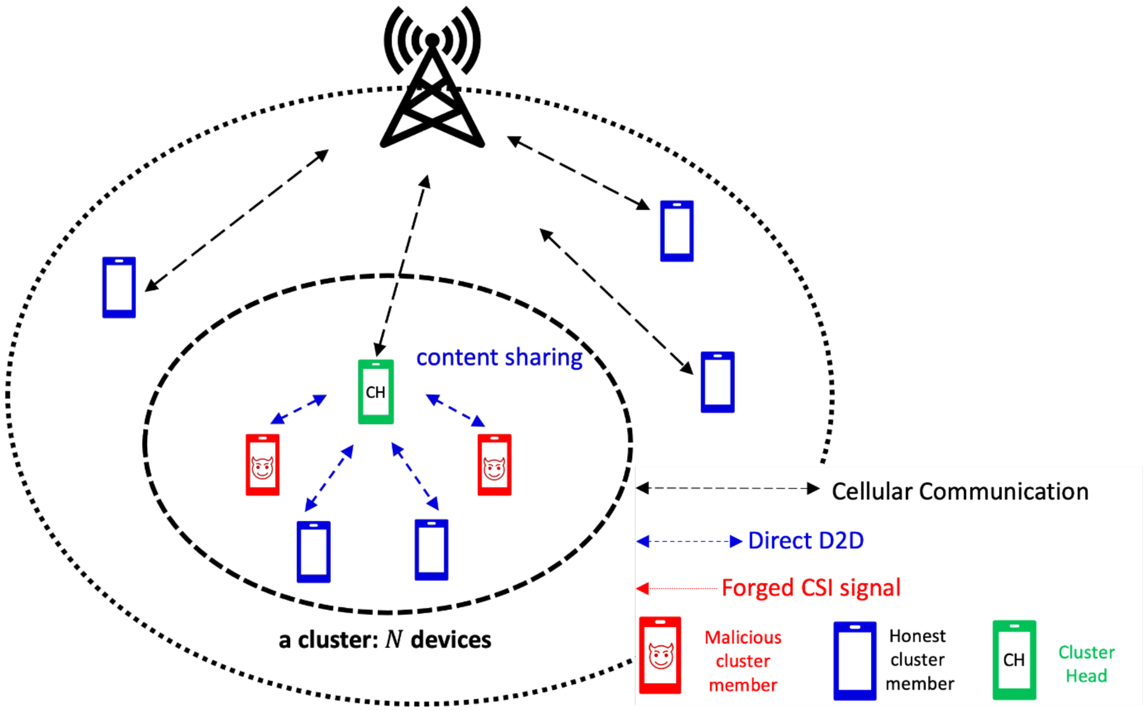
❑ Consider a cellular network

  ✓ A single cluster of N devices

    ○ H honest devices

    ○ M malicious devices

❑ Devices in the cluster leverage D2D communication for content sharing.

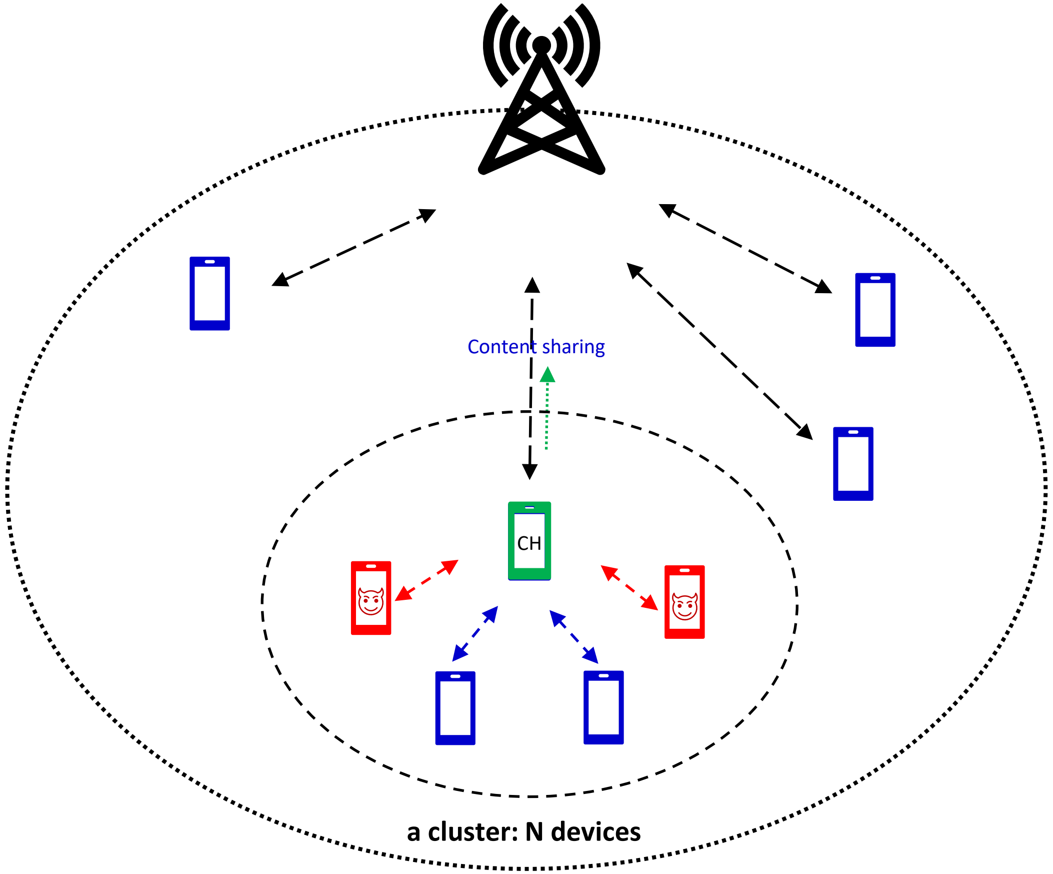


Threat Model (2/2)

❑ The main objective of the malicious devices is to degrade the performance of the whole cluster by:

- Reporting forged channel state information (CSI) to the base station to avoid selection as cluster heads.
- Reporting forged CSI to the chosen cluster head to reduce the minimum rate required for broadcast transmission of data in the cluster.
  - ✓ The reduction in the minimum data rate downs the performance of the cluster.

Forged CSI Attack (1/5)



Phase 1: Cluster Head Selection

Phase 2: Performance Degradation

Forged CSI Attack (2/5)

- **Phase I - Cluster Head Selection**
  - The malicious devices report forged CSIs to the base station to avoid selection as cluster heads.
  - NB: Being chosen as cluster heads means they cannot execute the attack.
  - The relationship between the true and forged CSI is expressed as:

$$\boldsymbol{f_n} = \boldsymbol{\beta}|\boldsymbol{g_n}|^{\mathbf{2}} \quad \dots\dots\dots\dots (1)$$

  - g_n denotes the true CSI of the malicious device and $\beta \in [0,1]$ is a forging factor.

Forged CSI Attack (3/5)

- Part of the total power allocated to devices for being cluster heads is wasted due to malicious devices reporting forged CSIs to the base station and avoiding the cluster head selection.
- The power that is wasted due to the forged CSI attack compared with the normal case is given as the ratio:

$$\boldsymbol{\alpha} = \frac{\boldsymbol{M}}{\boldsymbol{N} - \boldsymbol{M}} \quad \ldots\ldots\ldots\ldots(2)$$

Forged CSI Attack (4/5)

- **Phase II – Performance Degradation**
  - The cluster head requires the CSIs of the cluster members to deliver data to them.
  - The malicious devices in the cluster report forged CSIs to the cluster head.
  - The cluster head delivers content to the devices after receiving their CSIs.
    - ✓Assuming broadcasting mode of transmission
    - ✓Achievable rate is set with respect to the device with the worst CSI.
  - The cluster head broadcasts the data to the devices at the minimum data rate.

Forged CSI Attack (5/5)

- The minimum achievable rate to make sure all cluster members receive content is given by:

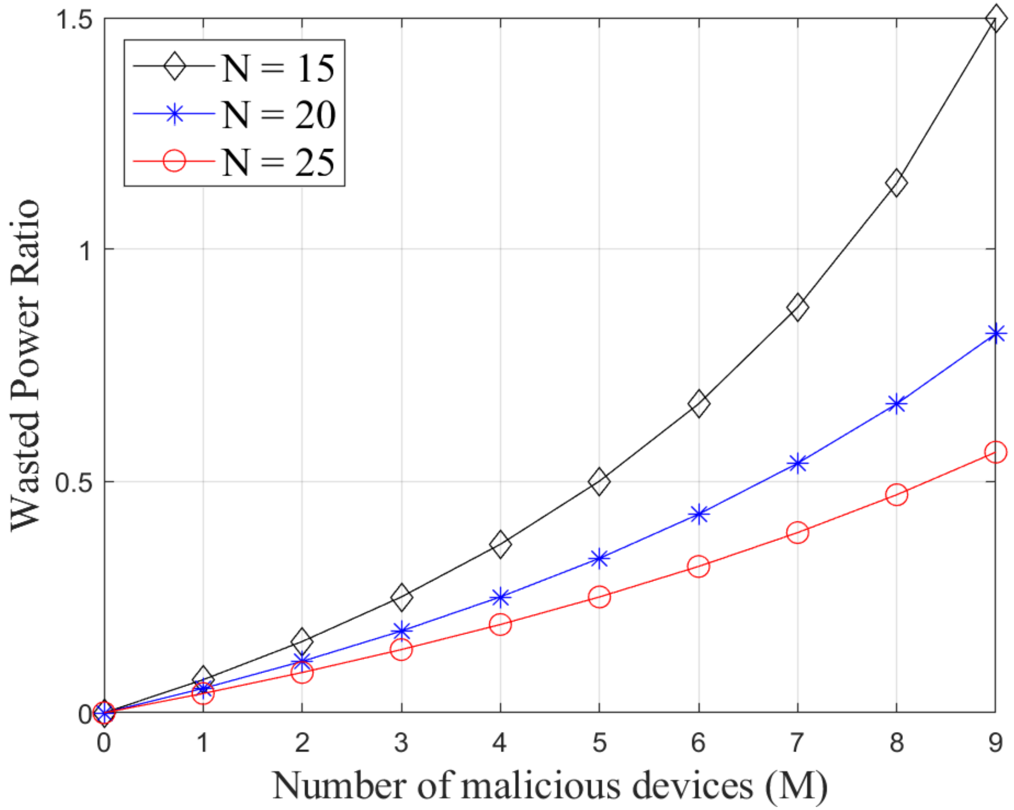
$$\boldsymbol{R_{min} = min\left[log_2\left(1 + |g_n|^2 SNR\right), log_2\left(1 + |f_m|^2 SNR\right)\right]} \ldots\ldots\ldots \quad (3)$$

- $|g_n|^2, |f_m|^2$ which represent the true and forged CSIs respectively, are assumed to follow Rayleigh fading channels.

- Equation (3) implies that if a forged CSI gives the minimum rate, the whole cluster suffers a performance degradation since forging factor is chosen by the malicious devices to give a low CSI.

Numerical Results

- **Wasted power ratio versus number of malicious devices**

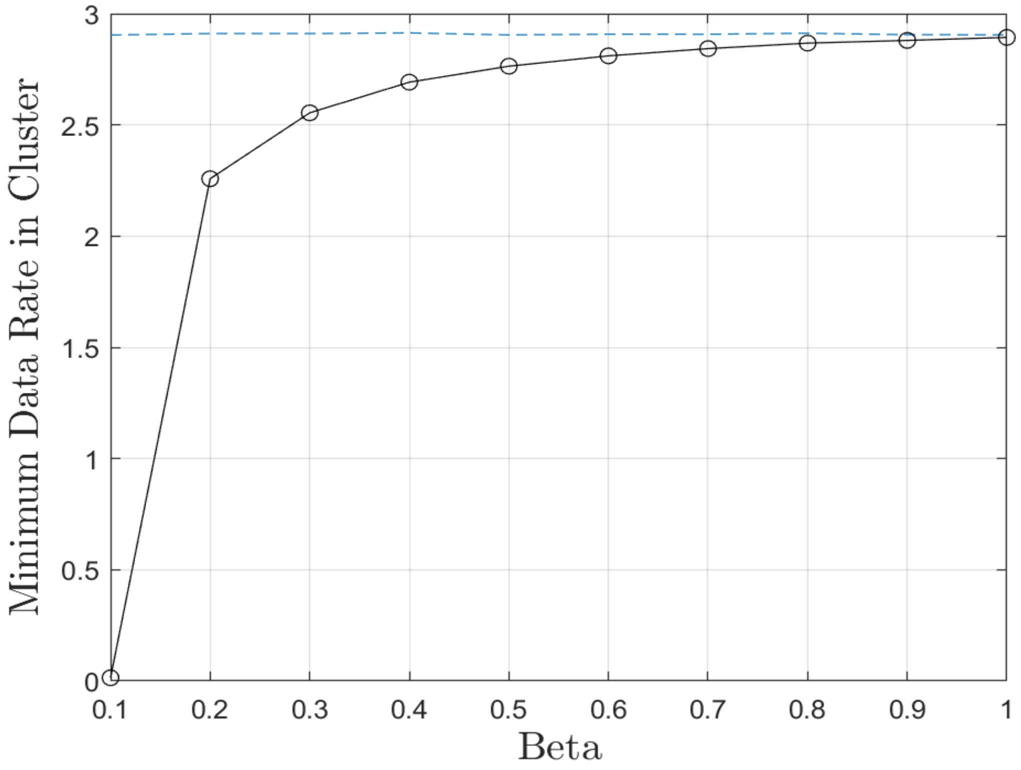


✓ The wasted power ratio represents the power wasted during the cluster head selection due to the presence of malicious devices.

✓ The power that is wasted increases with an increase in the number of malicious devices.

Numerical Results

- **Cluster performance with respect to forged CSI**



✓ We consider a forged CSI factor $\beta \in [0,1]$

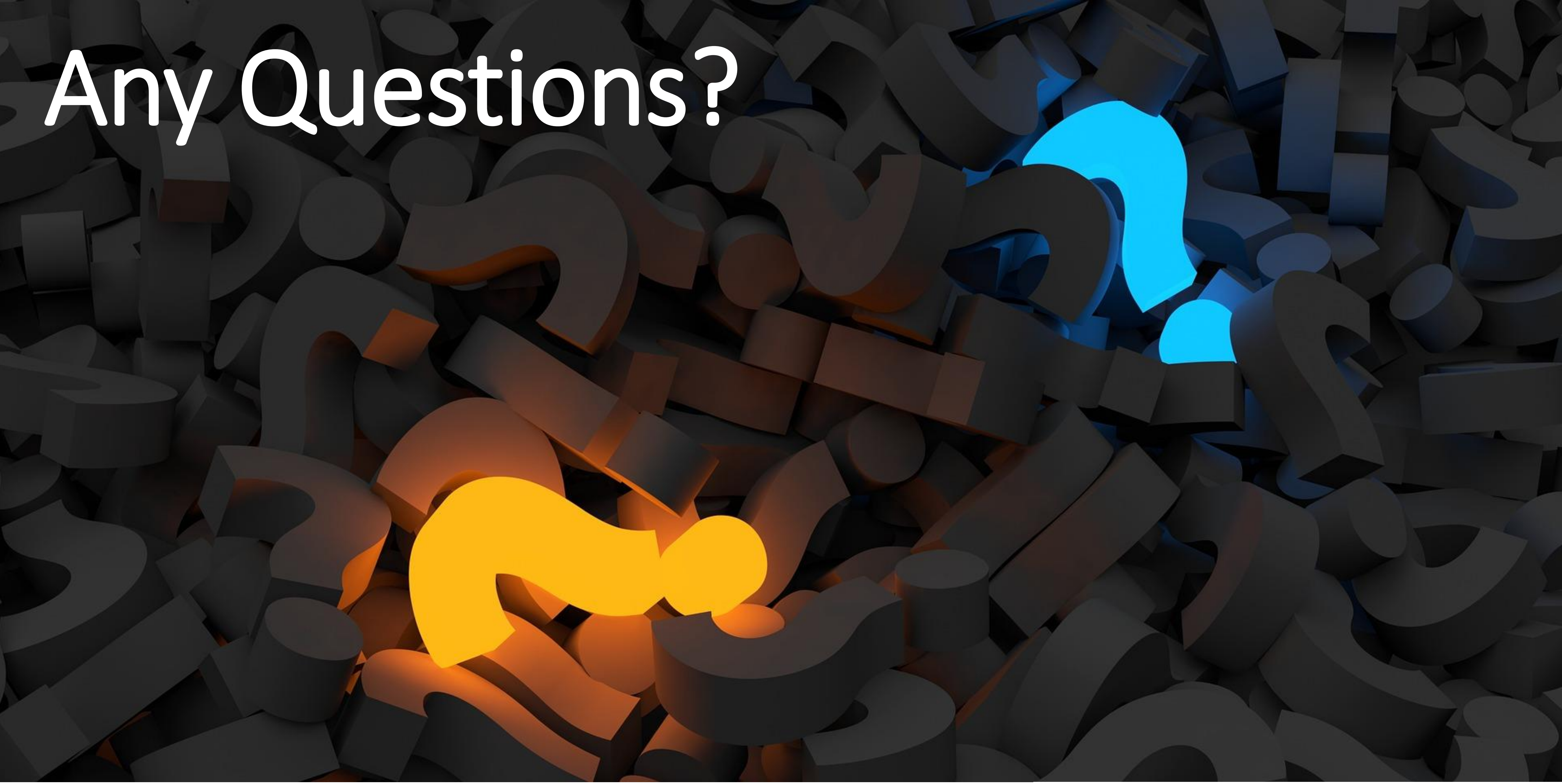
✓ The minimum data rate is the rate at which the cluster head broadcasts data to all the cluster members.

✓ We observe that the minimum data rate of the cluster reduces due to the transmission of forged CSI.

Conclusion

- We presented a potential threat of forged CSI attacks in **cluster-based D2D communication in cellular networks.**
- We analyzed **power wasted** in the selection of a cluster head
- We evaluate the impact of **forged CSI attacks** on the performance degradation in **data rate.**
- For future work, we can analyze the **detection of the forged CSI attack and the definition and probability of success of the attack.**

Any Questions?



HANBAT NATIONAL UNIVERSITY

E-mail: manyavenissa@gmail.com