Design of IR-HARQ-Based Network Coding for Secure Optical Satellite System

Luan Doan

Computer Communications Lab.

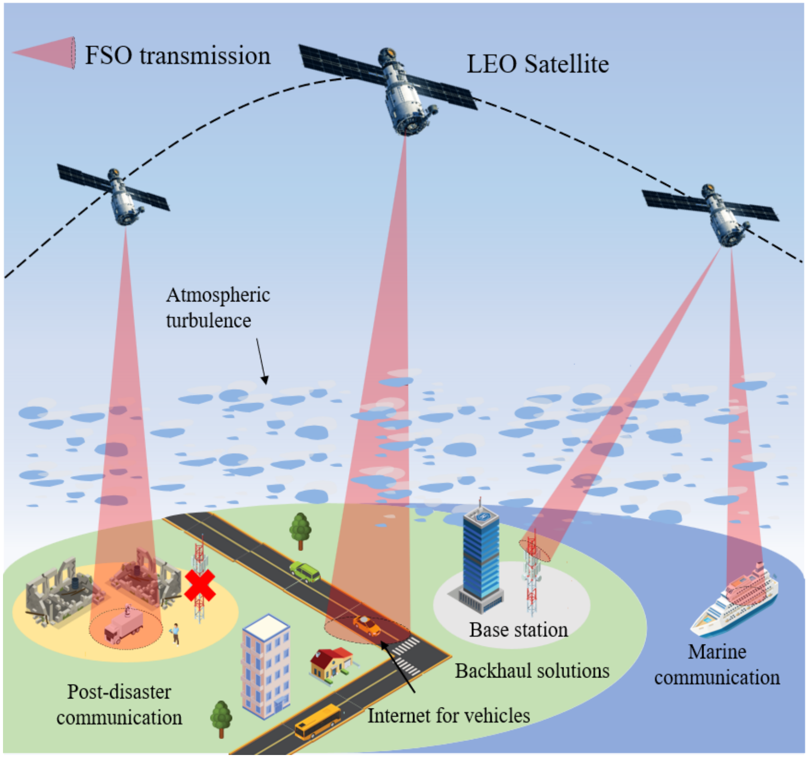
The University of Aizu

May. 14th, 2025

Outline of presentation

Free-Space Optics (FSO)-Based Satellite Systems

- **Free-space Optics (FSO):**
  - Infrared wavelength (700-1600nm)
  - Extremely high data rate (Gbps or even Tbps)
- **Low-earth Orbit (LEO) Satellite:**
  - Reduce latency compared to other satellites: LEO (160-2000km), MEO (2000- 35,786km), GEO (35,786km)
  - Provide global coverage through a constellation network => **provide internet access to remote areas**



➢ **FSO Based Satellite Systems** could be considered "keys“ in 6G infrastructure.

Problems in FSO-Based Satellite Systems

➤ **Unreliable transmission**

○ **Atmospheric turbulence:**

- Due to variations in temperature and pressure within the Earth's atmosphere **=> refractive index variations => distort the light => scintillation effect**
- **=>** results in signal power fluctuations at the receiver

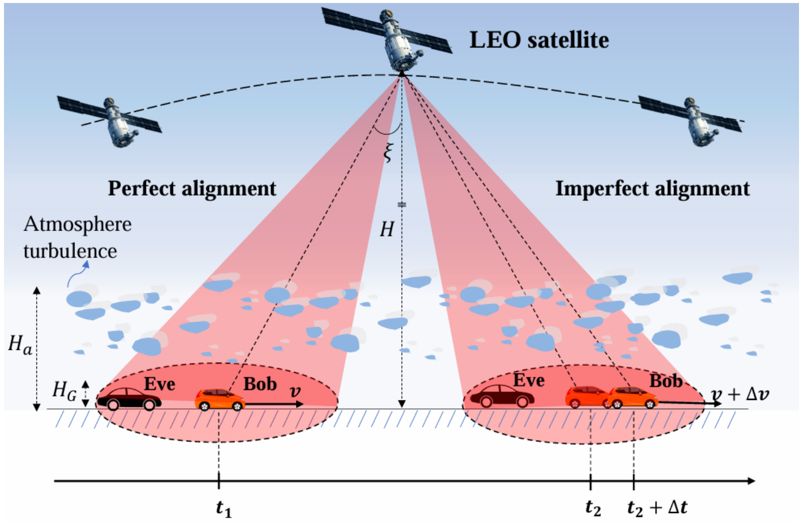
○ **Atmospheric attenuation :**

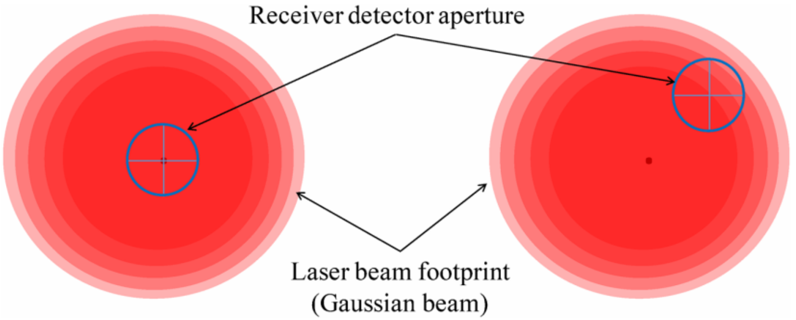
- Laser beam propagates through the atmosphere, it may interact with various gas molecules and aerosol particles
- => molecular **absorption** and **scattering** phenomenon
- **=> results in the attenuation of optical signal power**

○ **Pointing error:**

- Caused by the **vibration of LEO** satellite and **the sudden change in the velocity** of Bob
- Lead to the misalignment between the beam center and the detector center
- **=> Increases the geometric loss** (when considering the Gaussian beam)
- => **the receiver detector can only capture a fraction of power from the satellite**

=> HARQ is proposed for reliable transmission





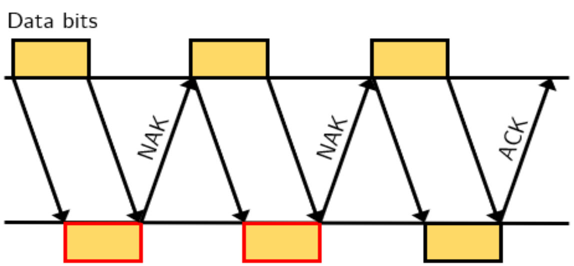
(a) (b)

(a) Without misalignment
(b) With misalignment between the centers of satellite beam footprint and receiver detector

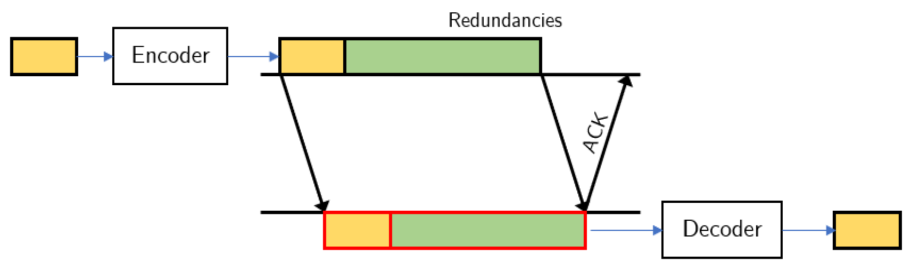
Hybrid ARQ (HARQ)

➢ Hybrid ARQ (HARQ): **A combination of ARQ and ECC** to **enhance reliable transmission**

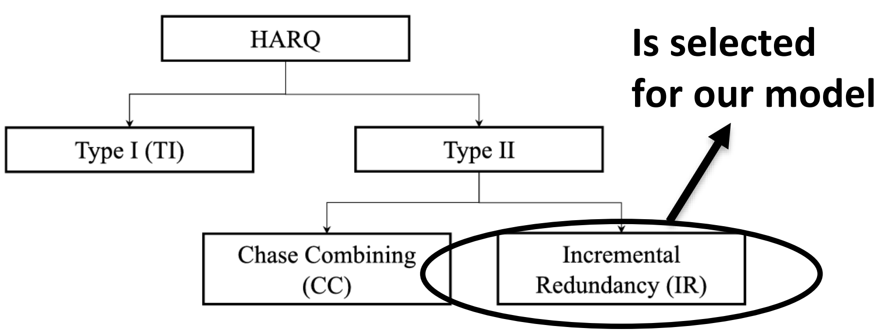
- **Automatic Repeat reQuest (ARQ)**
  - Retransmit erroneous frames



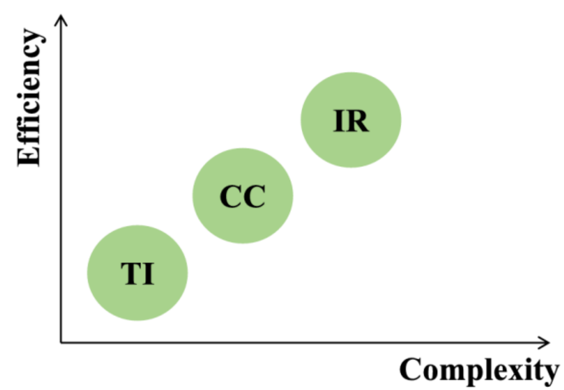
- **Error Correction Code (ECC)**
  - Add redundancy to the frame so that errors can be corrected at the receiver



HARQ Classification



Comparison of HARQ Types



Problems in FSO-Based Satellite Systems

- Consider the FSO communication from LEO satellite to Bob and Eve
  - Bob and Eve are internet of vehicles: self-driving cars
  - **LEO satellite transmit private data to Bob and Eve want to overhear it**
  - The channel is affected by atmospheric turbulence, atmospheric turbulence and pointing error

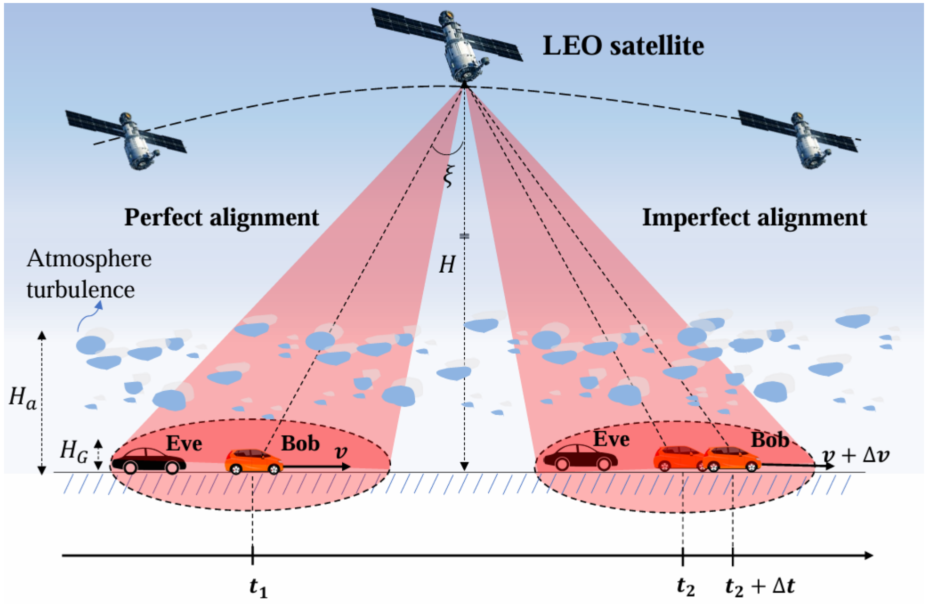


Fig. 1. An illustration of FSO-based satellite-assisted IoV systems in the presence of an eavesdropper.

➢ **The risk of security**
  - Presence of eavesdropper
  - The wider laser beam footprint
  - Retransmission of ARQ

➢ **To combat the risk of security => Propose HARQ-based network coding schemes to enhance the security and reliability of system**

Network Coding

- **Network coding** is employed to enhance the **transmission security** (per-frame level)

- **The private file** is divided into N original frames with $s = (s_1, s_2, \dots, s_N)$
- s is encoded to $F = (F_1, F_2, \dots, F_N)$

If N is odd

$$G = \begin{bmatrix} 1 & 1 & 0 & 0 & \dots & 0 & 0 \\ 1 & 0 & 1 & 0 & \dots & 0 & 0 \\ & & & & & & \\ 1 & 0 & 0 & 0 & \ddots & 0 & 0 \\ 1 & 0 & 0 & \dots & 0 & 1 & 0 \\ 1 & 0 & 0 & \dots & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & \dots & 1 & 1 \end{bmatrix}_{N \times N}$$

If N is even

$$G = \begin{bmatrix} 1 & 1 & 0 & 0 & \dots & 0 & 0 \\ 1 & 0 & 1 & 0 & \dots & 0 & 0 \\ & & & & & & \\ 1 & 0 & 0 & 0 & \ddots & 0 & 0 \\ 1 & 0 & 0 & \dots & 0 & 1 & 0 \\ 1 & 0 & 0 & \dots & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & \dots & 1 & 1 \end{bmatrix}_{N \times N}$$

Coding scheme: $F = G(mod2)s$

Where: G is a $mod-2$ $N \times N$ encoding matrix

If N is even

$$s_1 \oplus s_2 = F_1$$
$$s_1 \oplus s_3 = F_2$$
$$\vdots$$
$$s_1 \oplus s_N = F_{N-1}$$
$$s_2 \oplus s_3 \dots \oplus s_N = F_N$$

If N is odd

$$s_1 \oplus s_2 = F_1$$
$$s_1 \oplus s_3 = F_2$$
$$\vdots$$
$$s_1 \oplus s_N = F_{N-1}$$
$$s_1 \oplus s_2 \oplus \dots \oplus s_N = F_N$$

s are encoded F

$F = (F_1, F_2, \dots, F_N)$

Network Decoding

Example: - The private file comprises 4 frames $s = (s_1, s_2, s_3, s_4)$
- s are encoded to frames $F = (F_1, F_2, F_3, F_4)$

Coding scheme:
$F = G(mod2)s$

$$\begin{bmatrix} F_1 \\ F_2 \\ F_3 \\ F_4 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix} \times \begin{bmatrix} s_1 \\ s_2 \\ s_3 \\ s_4 \end{bmatrix}$$

$$s_1 \oplus s_2 = F_1$$
$$s_1 \oplus s_3 = F_2$$
$$s_1 \oplus s_4 = F_3$$
$$s_2 \oplus s_3 \oplus s_4 = F_4$$

Decoding scheme:
$s = [G(mod2)]^{-1} F$

$$\begin{bmatrix} s_1 \\ s_2 \\ s_3 \\ s_4 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{bmatrix} \times \begin{bmatrix} F_1 \\ F_2 \\ F_3 \\ F_4 \end{bmatrix}$$

$$F_1 \oplus F_2 \oplus F_3 \oplus F_4 = s_1$$
$$F_2 \oplus F_3 \oplus F_4 = s_2$$
$$F_1 \oplus F_3 \oplus F_4 = s_3$$
$$F_1 \oplus F_2 \oplus F_4 = s_4$$

=> Need $N-1$ frames to decode any of the frames $s_2, \ldots, s_N$

=> Needs N frames to decode s_1

=> The number of received frames $< N-1$, the receiver cannot decode any frames

- **Network coding** enhance the **transmission security** (per-frame level)

Outline of presentation

Proposed Designs

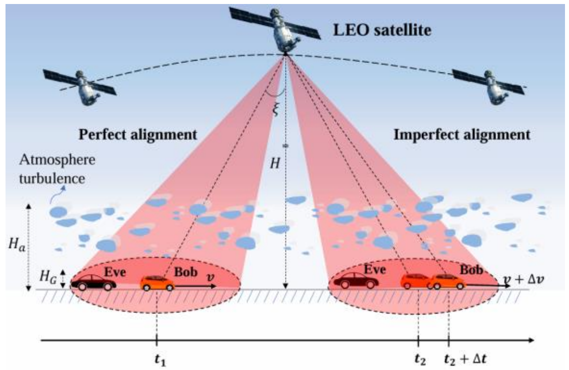
(1) Encoding Phase

⬇

(2) (Re)Transmission Phase

⬇

(3) Decoding Phase



System parameters

$Frame\ size = 3410\ bits$

$Bust\ size = 3000\ frames$=10.230.000 $bits$

$Network\ coding\ size = 100$ frames

$Fixed\ timeslot\ = 10.23\ ms$

$Mother\ code\ 1{:}\frac{1}{3},\ Family\ code{:}\ 1,\frac{1}{3},\frac{1}{3}$

$Mother\ code\ 2{:}\frac{1}{2},\ Family\ code{:}\ 1,\frac{11}{15},\frac{1}{2}$

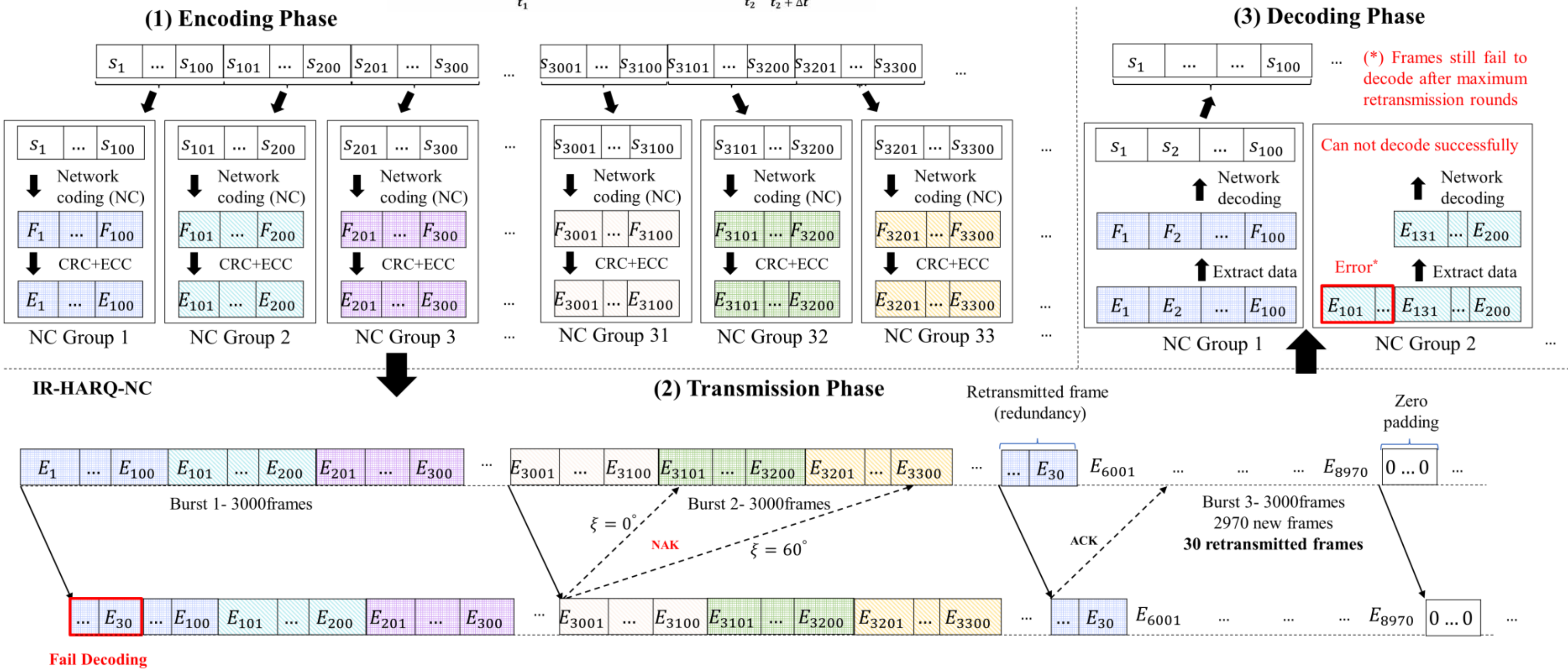


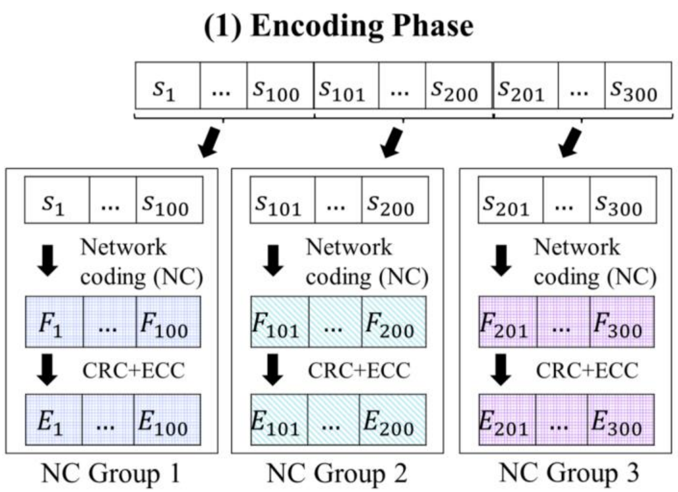
Fig.2. An illustrative example of the operation IR-HARQ-NC

Proposed Designs

(1) Encoding Phase

(2) Transmission Phase

(3) Decoding Phase



Network coding (NC)

Coding scheme:

$$F = G(mod2)s$$

$$s_1 \oplus s_2 = F_1$$

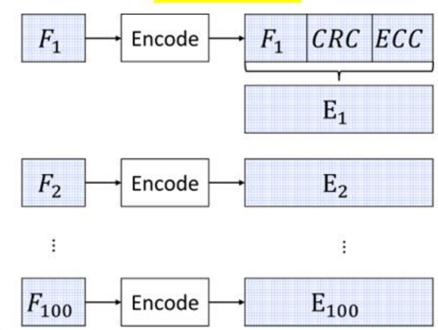
$$s_1 \oplus s_3 = F_2$$

$$\vdots$$

$$s_1 \oplus s_{100} = F_{99}$$

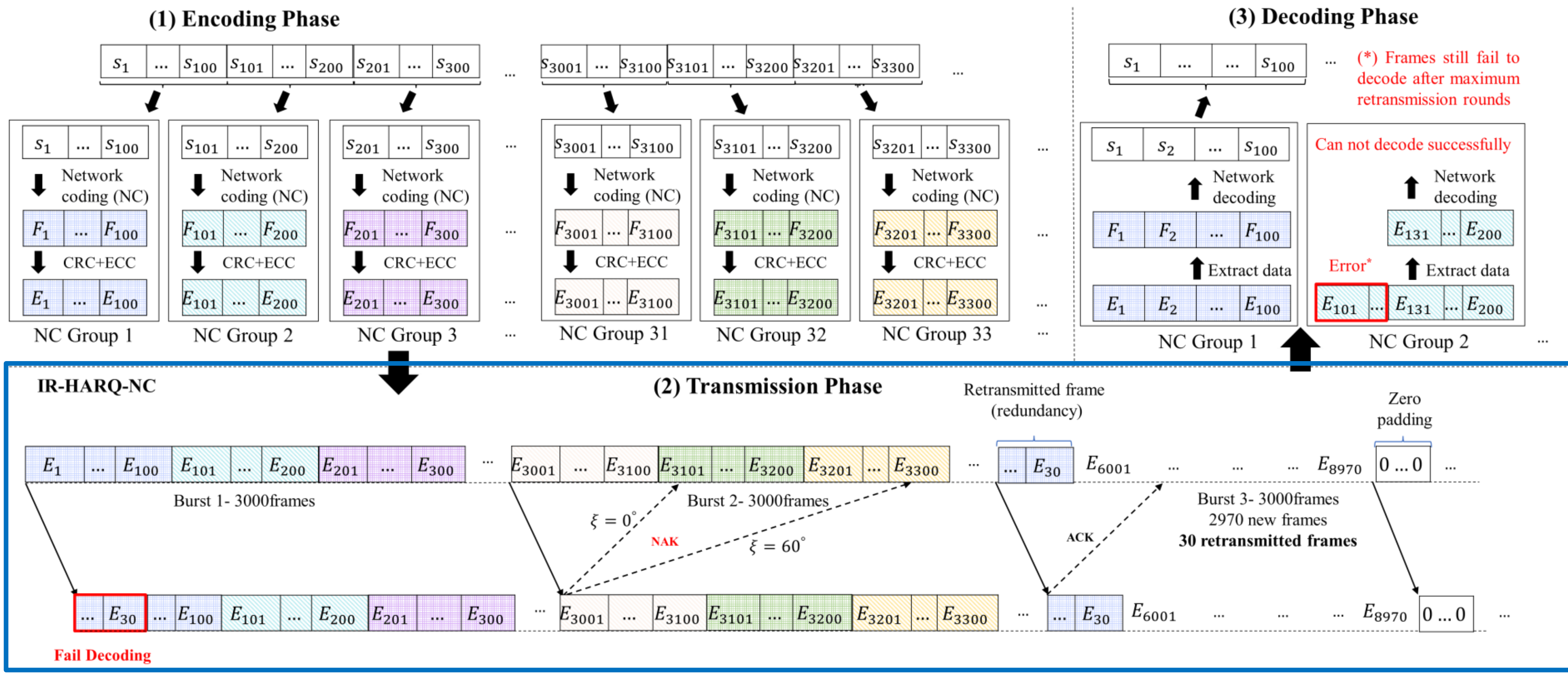
$$s_2 \oplus s_3 \oplus \ldots \oplus s_{100} = F_{100}$$

CRC+ECC



- The LEO satellite **applies network coding** to secure data frames before transmission by using the *encoding matrix G*
- To enhance reliability, network-coded frames are appended with a **CRC for error detection** and encoded using an **RS code for error correction**

Proposed Designs



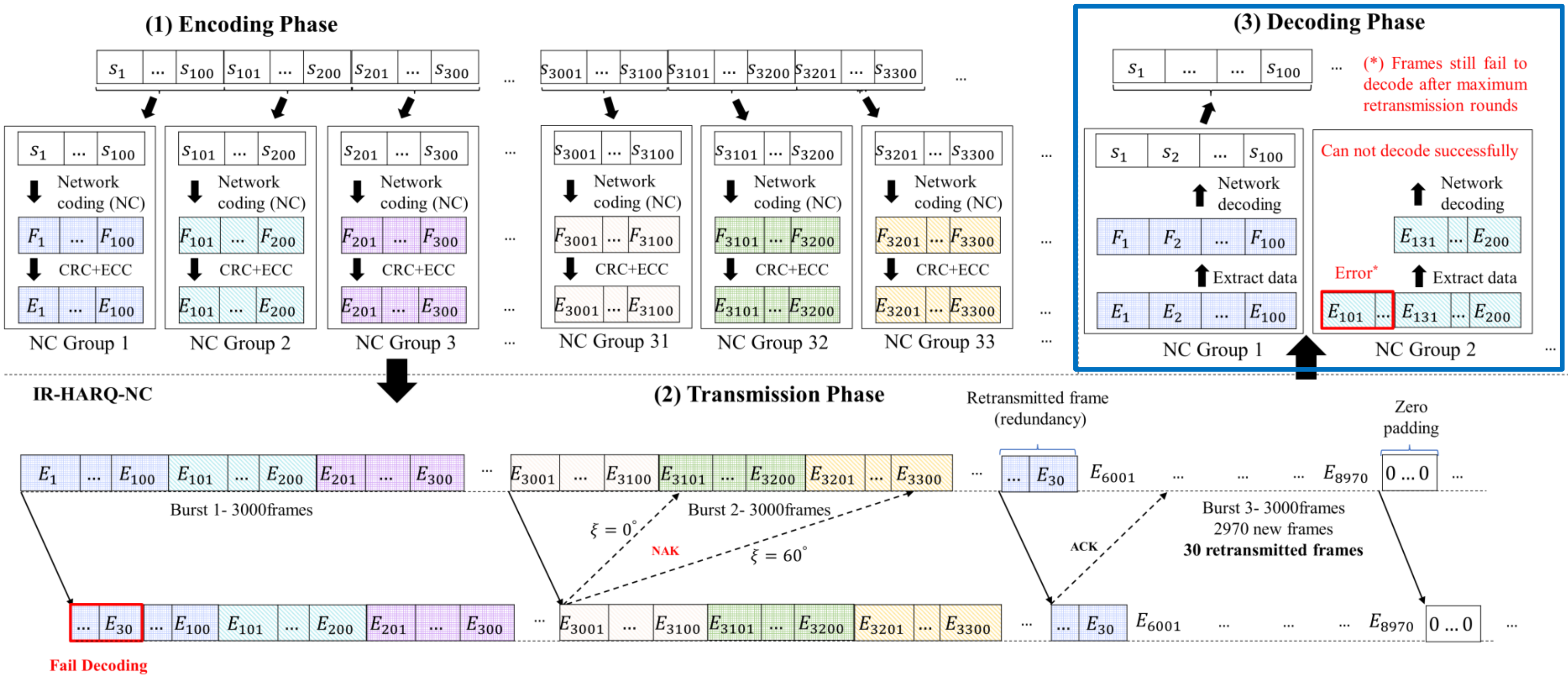
(1) Encoding Phase

(2) Transmission Phase

(3) Decoding Phase

- Each burst transmission will be transmitted in fixed time slot (10ms)
- One burst transmission contain frames from different network coding group
- Redundancy of erroneous frames will be transmitted right after next time slot until receiver decode successfully those frames of reaching the maximum retransmission

Proposed Designs



(1) Encoding Phase

⬇

(2) Transmission Phase

⬇

(3) Decoding Phase

- Bob can successfully decode the original frame s_k if all required network coded frames in the group are received
- With HARQ-NC, Bob can eventually decode all frames in a network coding group
- Eve may miss some frames, preventing her from reconstructing any data within the network coding group

Outline of presentation

Performance

➢ **Frame leakage probability, frame loss probability, goodput**

1. Frame leakage probability

If Eve received 1 network coding group with size N frames

- If Eve can decode successfully $N\ frames$ of this network coding group

$$P_{frame\ leakage\ probability} = \frac{N}{N} = 1$$

- If Eve can decode successfully $N-1\ frames$ of this network coding group

$$P_{frame\ leakage\ probability} \approx \frac{1}{N}$$

- If Eve can decode successfully fewer than $N-1$ frame of this network coding group

$$P_{frame\ leakage\ probability} = 0$$

If Eve received K network coding groups

- m: the number of network coding group that Eve can decode successful all frames (N) in each network coding group
- n: the number of network coding group that Eve can decode successful $N-1$ frames in each network coding group

$$P_{frame\ leakage\ probability} \approx \frac{m * 1 + n * \frac{1}{N}}{K}$$

Performance

2. Frame loss probability

If Bob received 1 network coding group with size N frames

- If Bob can decode successfully $N\ frames$ of this network coding group

$$P_{frame\ loss\ probability} = 1 - \frac{N}{N} = 0$$

- If Bob can decode successfully $N - 1\ frames$ of this network coding group

$$P_{frame\ loss\ probability} \approx 1 - \frac{1}{N} \approx \frac{N-1}{N}$$

- If Eve can decode successfully fewer than $N - 1$ frame of this network coding group

$$P_{frame\ loss\ probability} = 1$$

If Bob received K network coding groups

- m: the number of network coding group that Bob can **decode successfully fewer than $\boldsymbol{N}$–1** in each network coding group
- n: the number of network coding group that Bob can **decode successful $\boldsymbol{N-1}$ frames** in each network coding group

$$P_{frame\ loss\ probability} \approx \frac{m * 1\ +\ n * \dfrac{N-1}{N}}{K}$$

3. Goodput

If Bob decoded successfully $\boldsymbol{N}$ frames in $\boldsymbol{t\ time\ slots}$

$$Goodput = \frac{N * number\_of\_information\_bits\_per\_frame}{t}$$

Numerical Results And Discussion

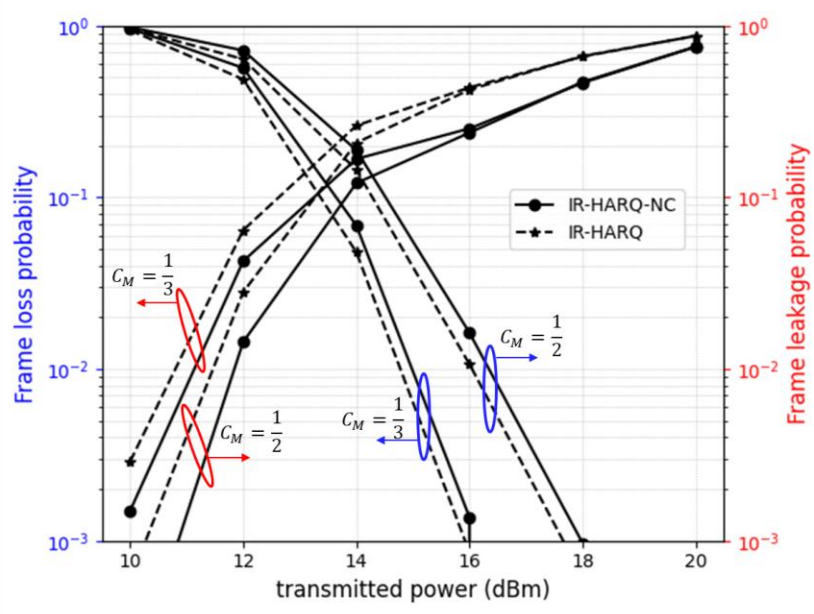


Fig.1. Performance comparison vs. different transmitted power levels.

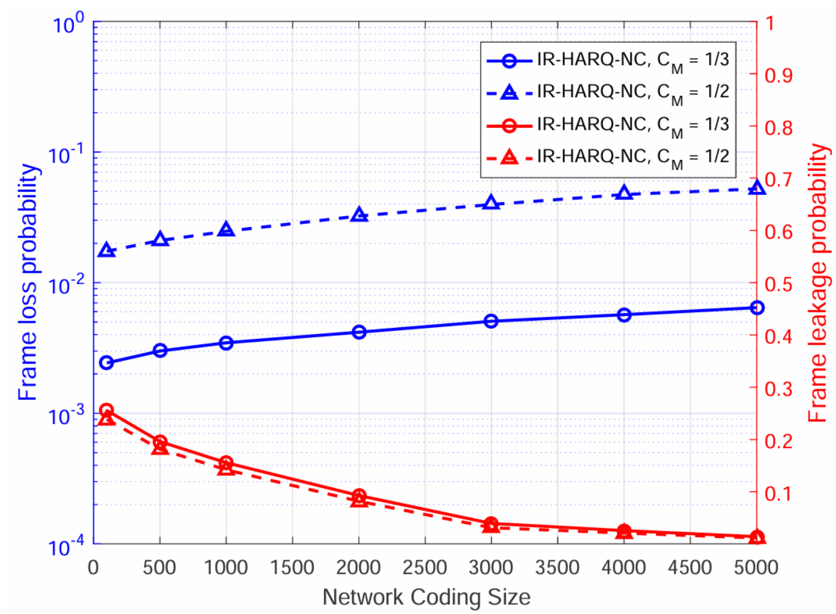


Fig.2. The intercept and outage probabilities vs. network coding size.

- The **security enhancement** comes at the cost of an **increased frame loss probability**
- It is importance to **select an appropriate transmitted power level** to achieve a targeted performance balance

- **A larger network coding group size enhance security**. However, this also leads to an **increase in frame loss probability**

Numerical Results And Discussion

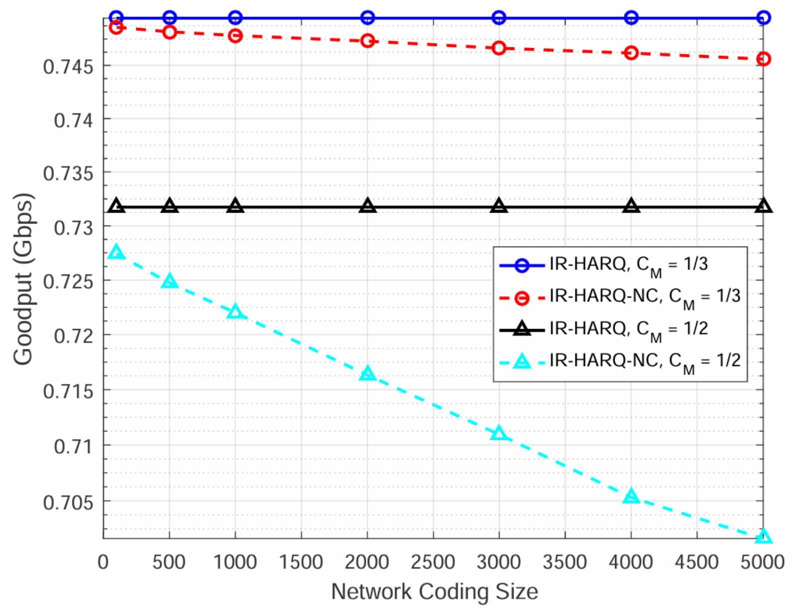


Fig.3. Goodput with different network coding size

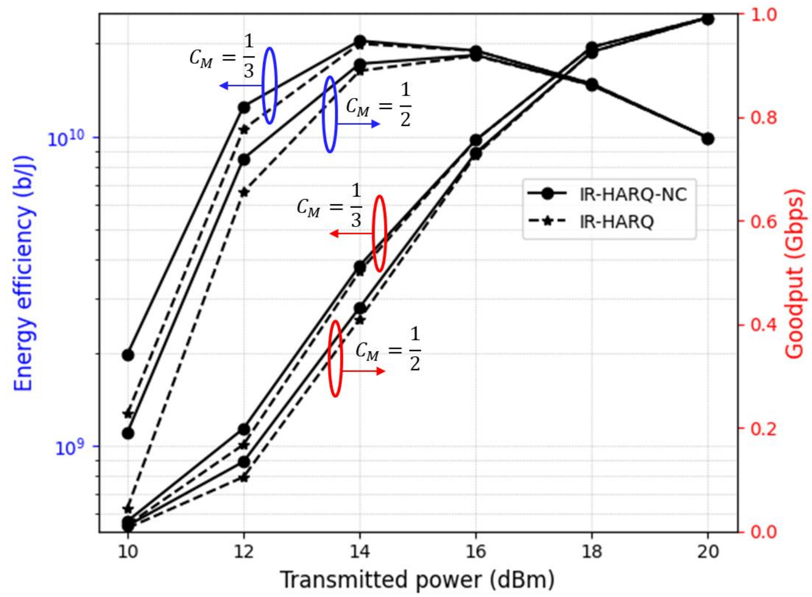


Fig.4. Energy efficiency and goodput with different transmitted power levels.

- IR-HARQ provide better goodput than IR-HARQ-NC for each code rate
- Larger sizes reduce goodput and the goodput of IR-HARQ-NC with $Mother\ code = 1/2$ decrease more significantly than that of IR-HARQ-NC with $Mother\ code = 1/3$

- Selecting optimal transmitted power levels can balance goodput and energy efficiency
- Using IR-HARQ-NC with $Mother\ code = 1/3$ can provide the system with higher energy efficiency and better throughput

Outline of presentation

Conclusion

- **Limitation of the system model**
- The model does not consider channel coherent time follow the change of LEO satellite's position
- The security of the model is not significantly improved

- **Plan for the next step**
- Consider channel coherent time follow the change of LEO satellite's position
- Improve the security of the system
- Apply a theoretical framework
- Consider NOMA-HARQ for the system

Thank you for your listening!