INL/MIS-19-54166-Revision-0

An Innovative Secure mmWave M2M Communication Network for Operating Drones

June 2019

Arupjyoti Bhuyan

DISCLAIMER

This information was prepared as an account of work sponsored by an agency of the U.S. Government. Neither the U.S. Government nor any agency thereof, nor any of their employees, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness, of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the U.S. Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the U.S. Government or any agency thereof.

INL/MIS-19-54166-Revision-0

An Innovative Secure mmWave M2M Communication Network for Operating Drones

Arupjyoti Bhuyan

June 2019

Idaho National Laboratory
Idaho Falls, Idaho 83415

http://www.inl.gov

Prepared for the
U.S. Department of Energy
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517

www.inl.gov
Idaho National Laboratory

An Innovative Secure mmWave M2M Communication Network for Operating Drones

Arupjyoti (Arup) Bhuyan (INL), Ismail Guvenc, Huaiyu Dai (North Carolina State University)

Need and Significance

- Use of UAVs (Unmanned Aerial Vehicles)/drones for non-military applications (e.g. public safety) is advancing rapidly in the U.S. In parallel, 5G is starting to transform the wireless networks across the world.
- Currently cellular drones utilize wireless networks optimized for ground coverage, that leaks into space for about 400 feet high.
- This research aims to validate that 5G millimeter wave (mmWave) beams with antenna arrays electronically tilted for optimal RF coverage in the sky can be used securely for drones.
- Successful conclusion will lead to higher security, reliability, and spectral efficiency than those achieved with current wireless networks for drone operation.

Approach and Innovative Aspects

- Analyze RF (Radio Frequency) coverage in the sky with the innovative use of mmWave phased arrays aimed towards the drone corridor to harness the power of 5G – multiplicative improvement in data throughput & reduction in latency, and support of massive M2M communications.
- Apply MA (Multiple Access) technology to increase the spectral efficiency by covering a swarm of drones with a single mmWave beam and associated radio resources.
- Design energy efficient low-bit quantization to form mmWave beams for drone operation.
- Use drones' navigation capabilities to significantly improve security by e.g. evading attackers.
- Utilize intra-drone communication to improve reliability as well as security.
- Demonstrate the simulated recovery of a critical infrastructure such as a power grid that requires a black restart with mmWave modeling and experiments .

Publications

1. "SLNR Based Precoding for One-Bit Quantized Massive MIMO in mmWave Communications," in Proc. IEEE Conference on Communications (ICC), May 2019 , STIMS #INL/CON-19-52778.
2. "Energy Efficiency of RSMA and NOMA in Cellular-Connected mmWave UAV Networks," in Proc. IEEE Conference on Communications (ICC), May 2019, , STIMS #INL/CON-9-52776.
3. "Interference avoidance UAV assisted networks: Joint 3D trajectory and power optimization," submitted to IEEE Global Communications Conference (GLOBECOM), Dec. 2019, STIMS #INL/CON-19-54017
4. "Physical layer security for mmWave drone links with NOMA," in 5th NSF Millimeter-Wave (mmWave) RCN Workshop, Jan. 2019 Journal paper to be submitted , "NeuralWave: Gait-based Human Recognition using Commodity WiFi and Deep Learning", May 31, 2018, STIMS #INL/CON-18-52279
5. Enhancing physical layer security for NOMA transmission in mmWave drone networks," in Proc. IEEE Asilomar Conference on Signals, Systems, and Computers, Pacific Grove, CA, Oct. 2018, STIMS #INL/CON-18-52261.

Current Results

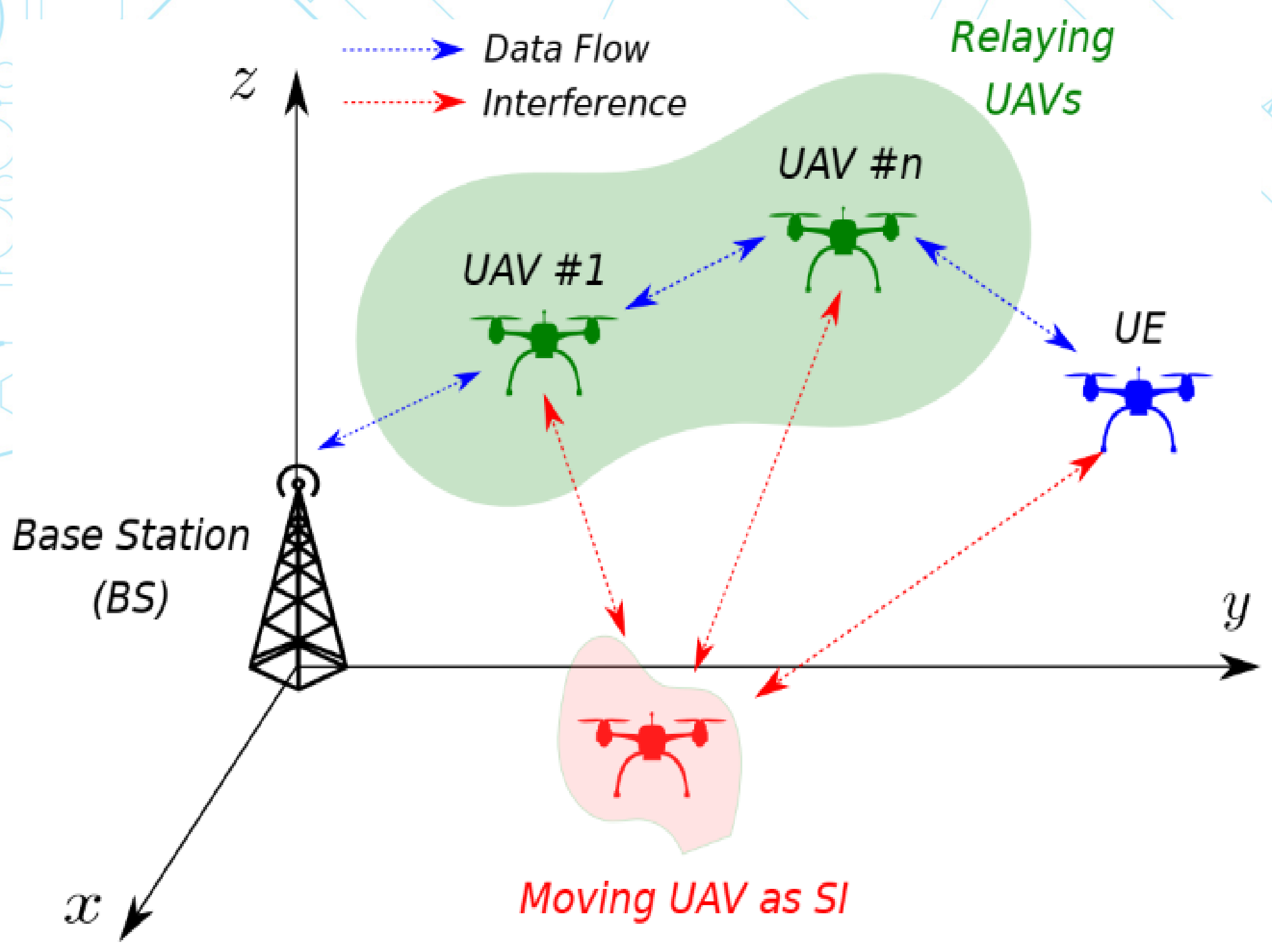

Fig. 1 System model for malicious drone attack on drone wireless network.

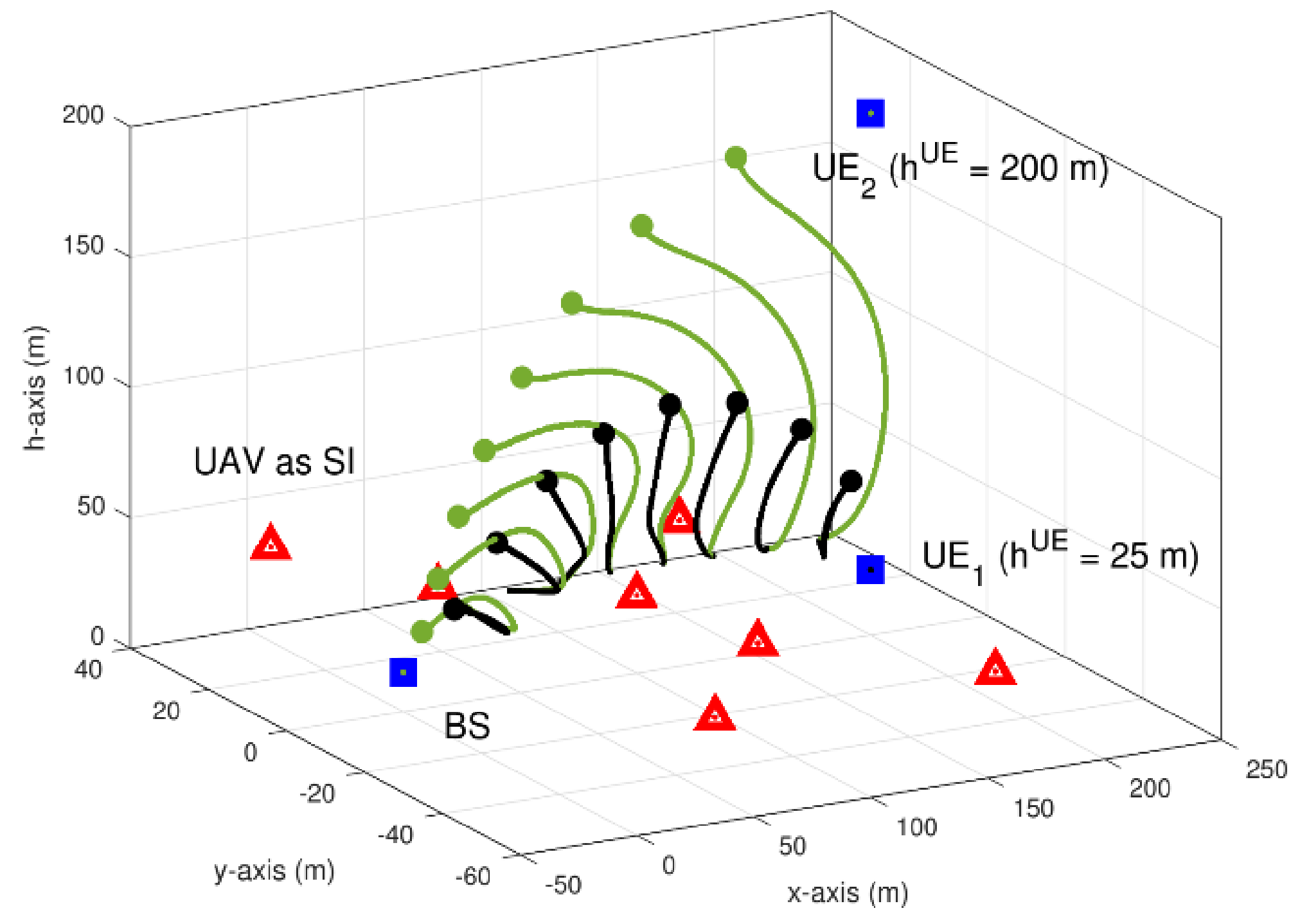

Fig. 2 3D view of optimized trajectories to avoid a malicious attack (e.g., jamming from ground).

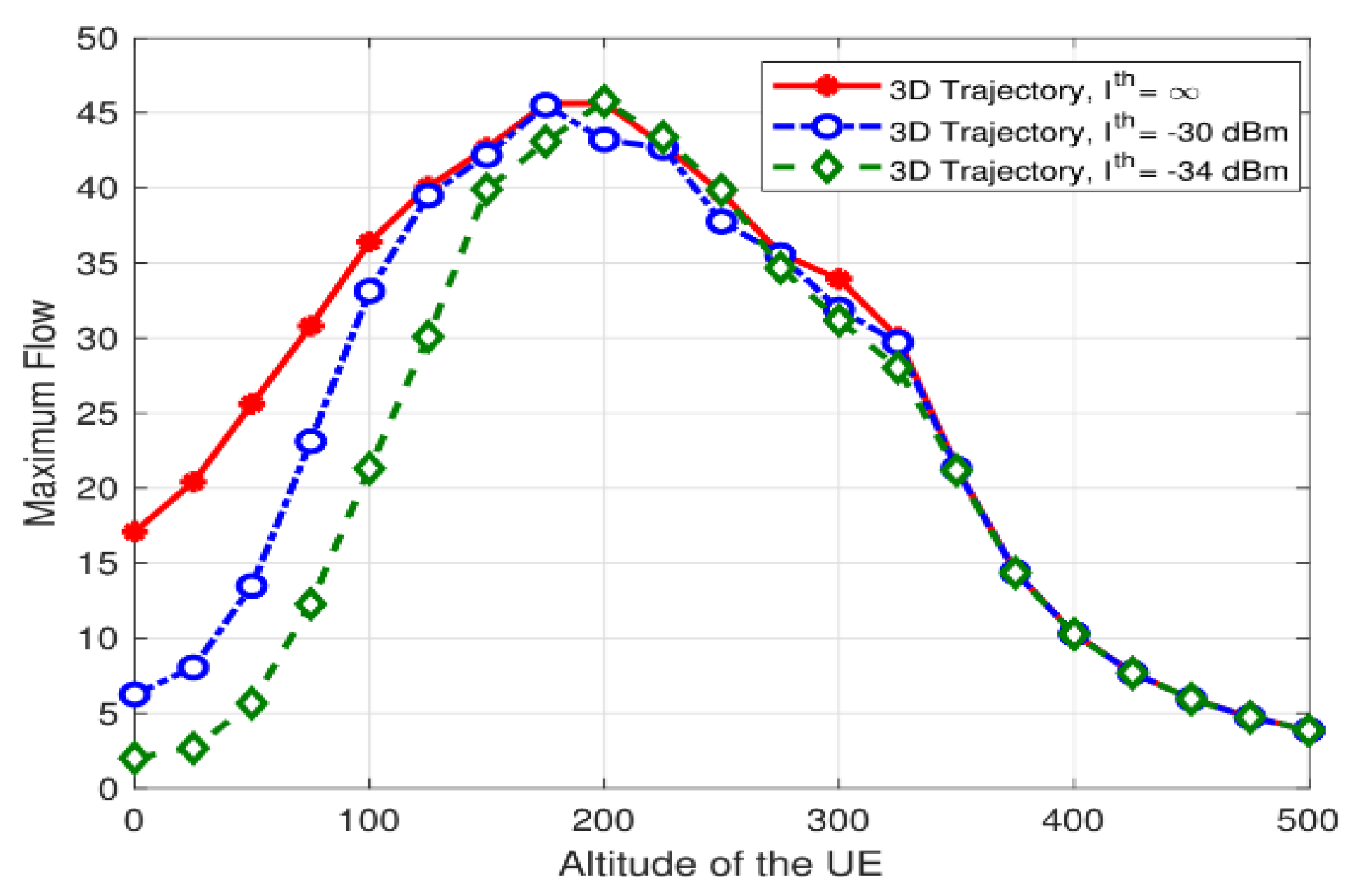

Fig. 3 Maximized data flow as a function of the recipient drone's height.

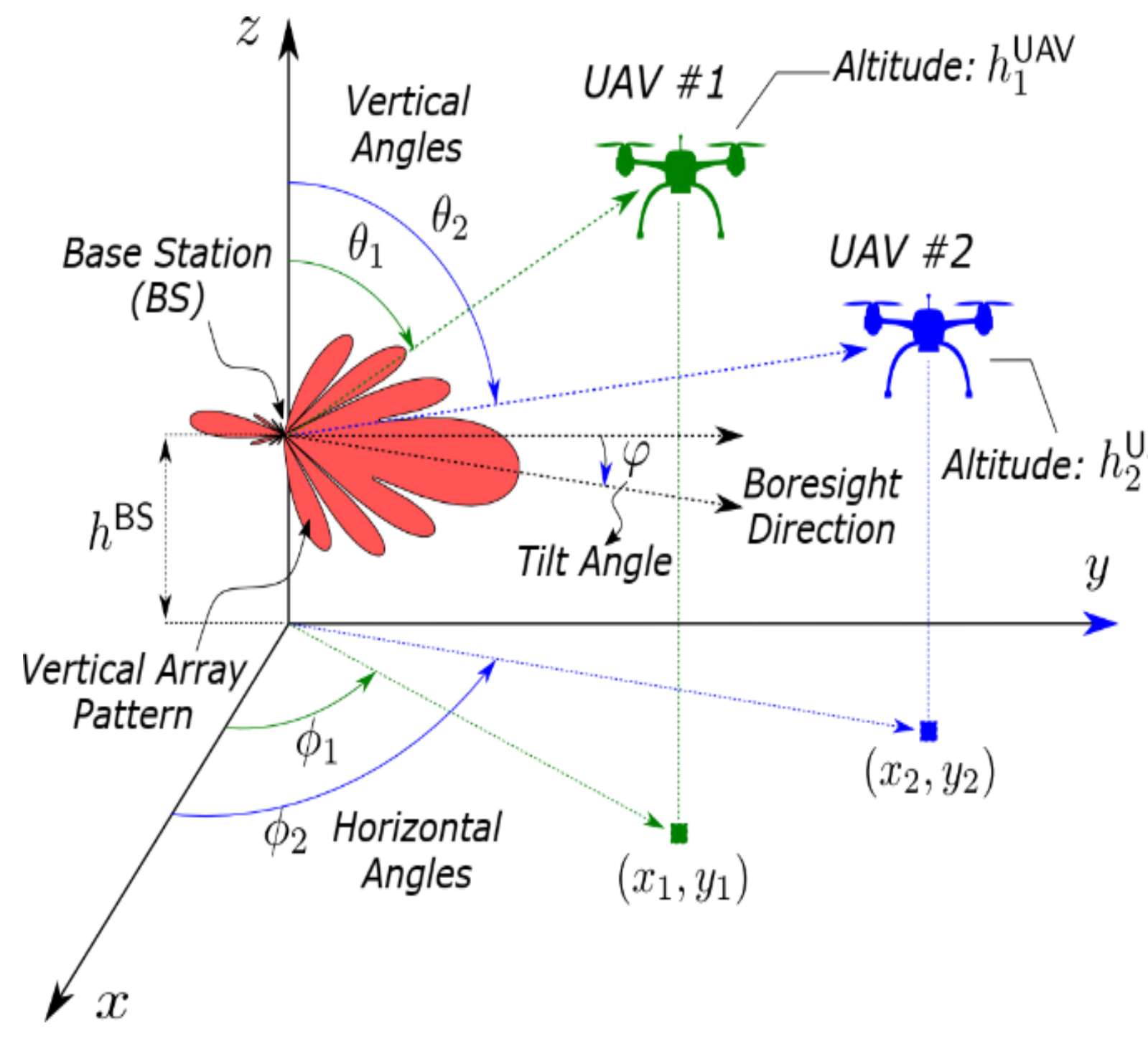

Fig. 4 System model for mmWave serving multiple drones simultaneously with an 8-element antenna array.

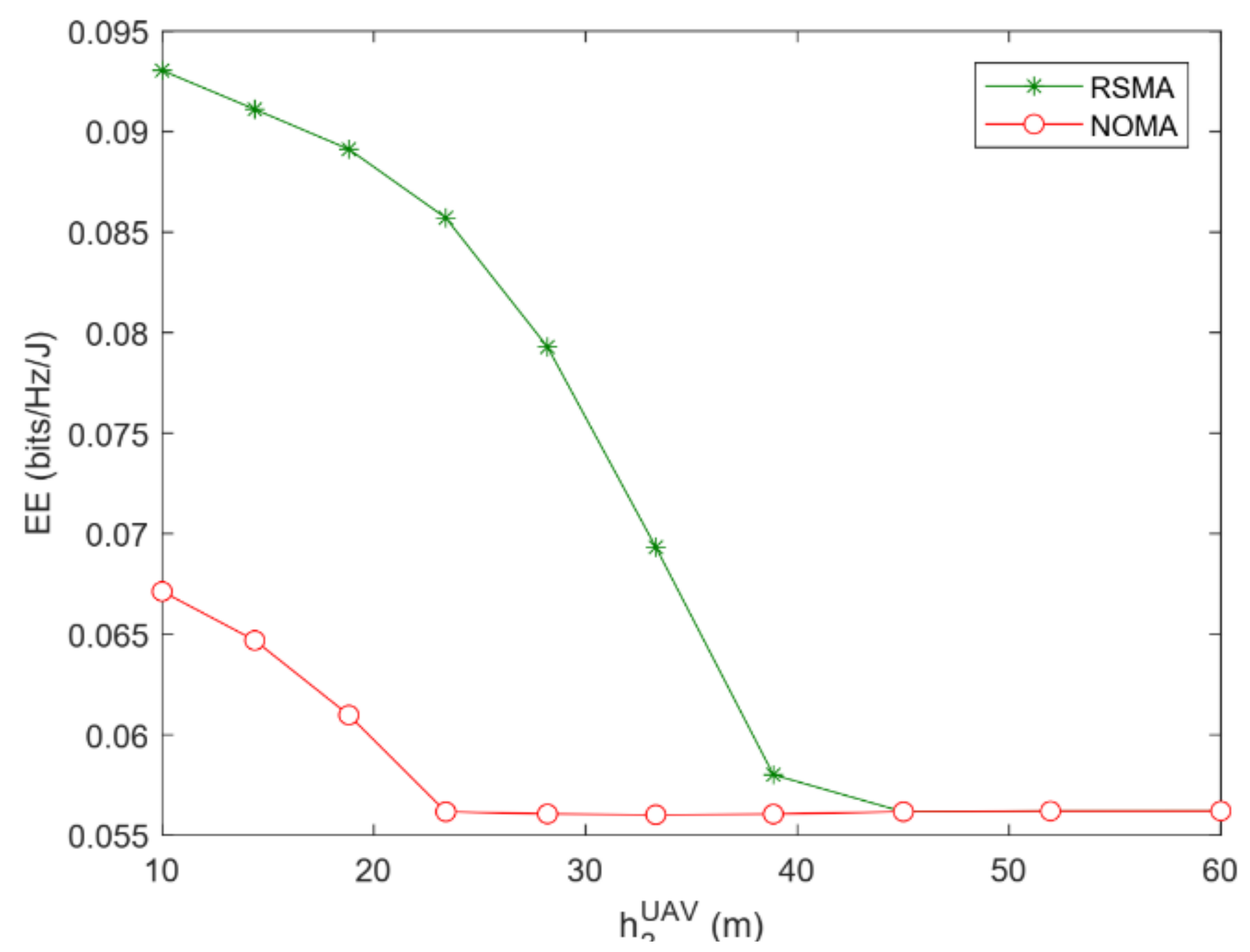

Fig. 5 Sum energy efficiency versus the altitude of the 2nd UAV served with RSMA and NOMA.

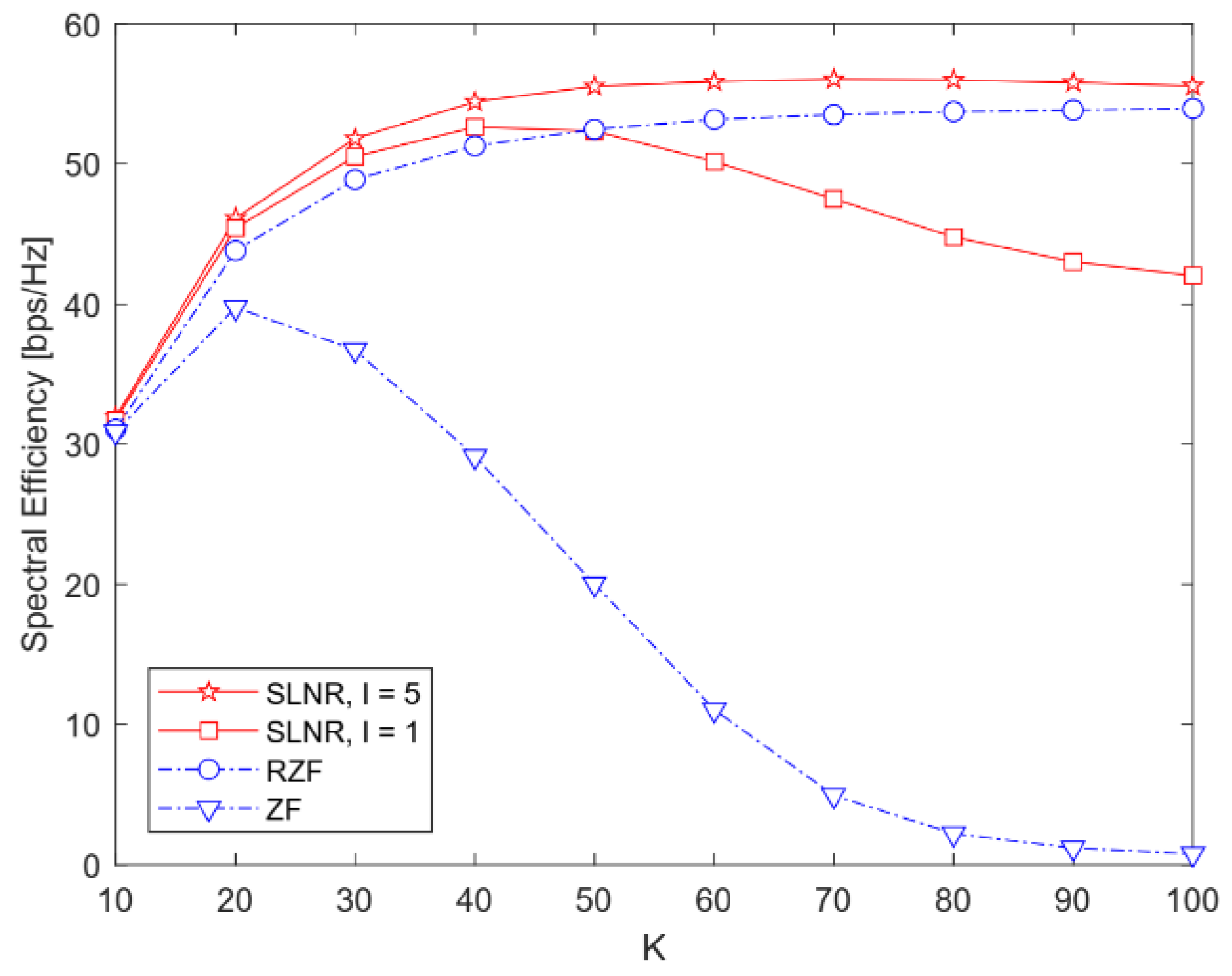

Fig. 6 Spectral efficiency vs number of users (K) at 10 dB SNR (RZF and ZF are conventional).