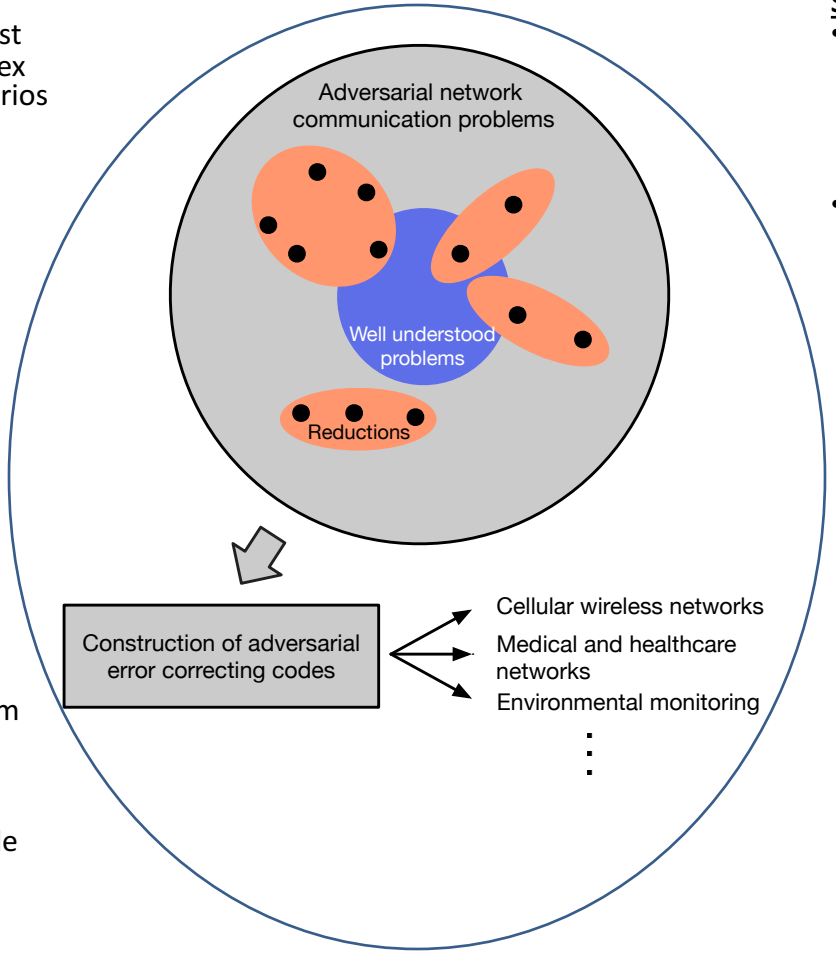
Communication under Adversarial Attacks in Complex Networks - Fundamental Limits and Secure Coding Strategies

NJIT New Jersey's Science & Technology University

Challenge:

- To study coding schemes against adversaries in emerging complex network communication scenarios and new tools to assess their fundamental limits.
- Adversarial actions include jamming, Byzantine attacks, distributed Denial-of-Service attacks.



Taxonomy of adversarial network communication problems and applications

Scientific Impact:

- Existing work on secure and reliable network communication has focused mostly on academic cases (notably the uniform-link single-source multicast scenario).
- Limited more practical generalizations beyond these settings (i.e., multiple sources, non-uniform adversarial sets, delay requirements) have not been sufficiently addressed and lead to significantly different theory.

Solution:

- Information-theoretic security-performance trade-off obtained via novel reductions, which transform one hard-to-solve network communication problem into an equivalent one which is easier to solve.
- Fundamental limits provide performance guarantees for code design.

Broader Impact:

- Advancing information technology and its benefits to society through newly established theory and practice of security under adversarial attacks for multiple sources and terminals.
- Impact on fields where reliable networking Is required, e.g., in the fields of cellular communication, healthcare, environmental monitoring, finance, etc.
- Impact on underrepresented communities (a female Ph.D. student has been hired on the project).

CNS-1526547, New Jersey Institute of Technology, Contact: Prof. Joerg Kliewer, jkliewer@njit.edu