# Review and Evaluation of Security Threats on the Communication Networks in the Smart Grid

Zhuo Lu, Xiang Lu, Wenye Wang, Cliff Wang*

Department of ECE,
North Carolina State University

*Army Research
Office, RTP, NC

The work is sponsored by the NSF Future Renewable Electric Energy Delivery and Management (**FREEDM**) Systems Center and the ARO secure open systems initiative (**SOSI**).

# Outline

- **Background and Motivation**
  - **Why Smart Grid?**
- **A glance of the smart grid and security**
  - **Architecture of the smart grid communication network**
  - **Classification of security threats**
- **A case study for traffic-flooding attacks.**
  - **A mini-showcase of  the smart grid communication network**
  - **Delay performance measurement**
- **Conclusion**

# Networks in our daily life

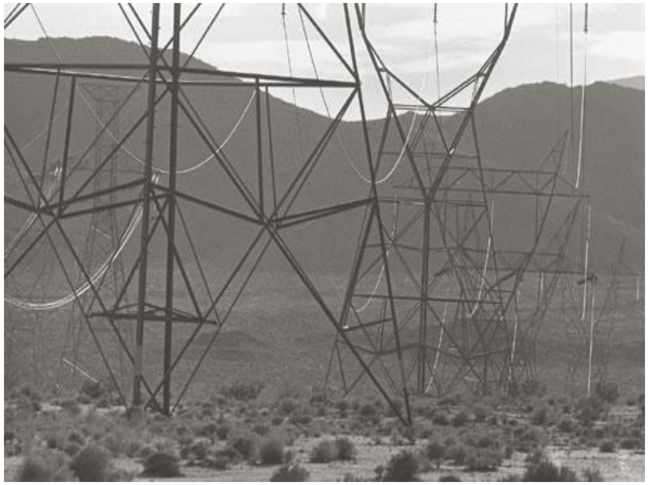
- Evolution of information technology
  - the Internet paradigm

30 years ago

Today

# Why Smart Grid?

- Evolution of power grids



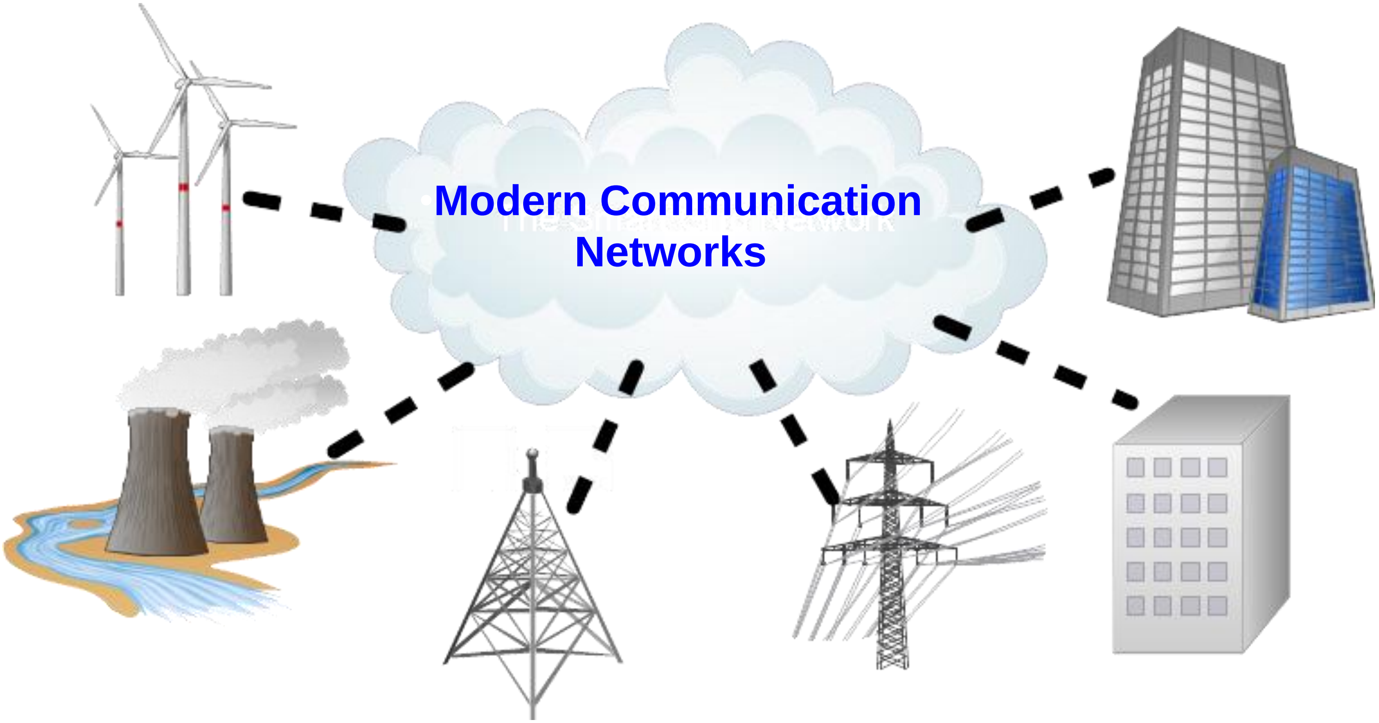
30 years ago

Today

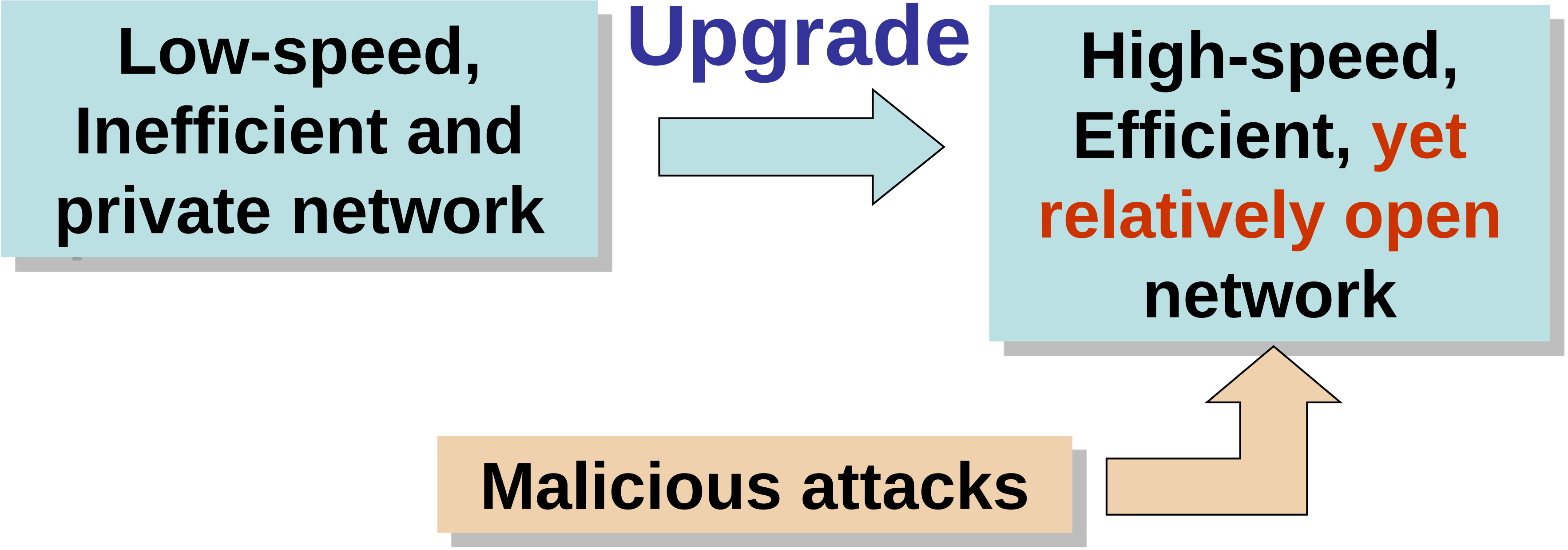
- Smart grid: the next-generation power system. (Energy Internet!)
  – On Oct. 27 2009, the Obama Administration announced 100 grants, totaling $3.4 billion, for smart-grid efforts.

# Smart Grid Communication Networks

- **The smart grid is a new paradigm for energy management and delivery systems.**
  - **Advanced digital computing and networking system connects every single part of the grid.**



# Network Security in the Smart Grid



Low-speed, Inefficient and private network

Upgrade

High-speed, Efficient, yet relatively open network

Malicious attacks

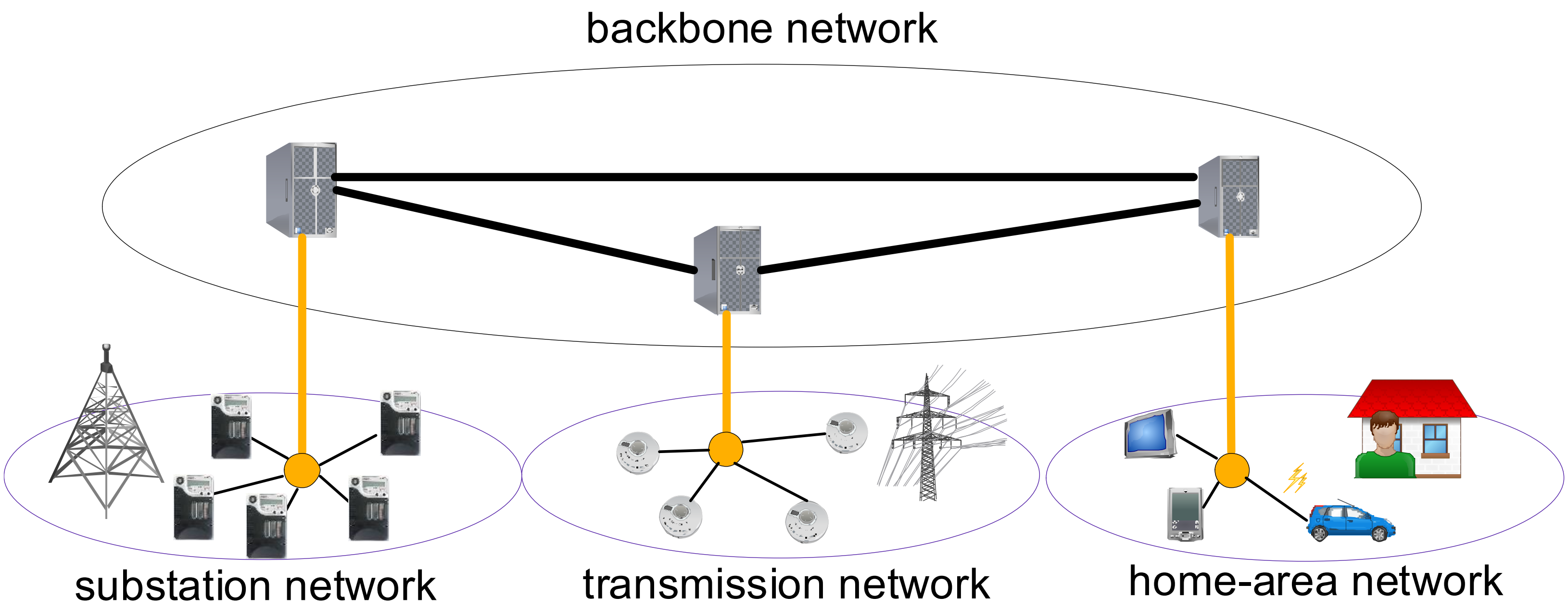
- In this work, we
  - take a quick glance at network security threats in the smart grid;
  - use a simple case study to illustrate the attack impact on power networks

# Outline

- Background and Motivation
- A glance of the smart grid and security
  - Architecture of the smart grid communication network
  - Classification of security threats
- A case study for traffic-flooding attacks.
- Conclusion

# Fundamental Architecture

- **Hierarchical architecture.**
  - **Backbone network and local-area networks**



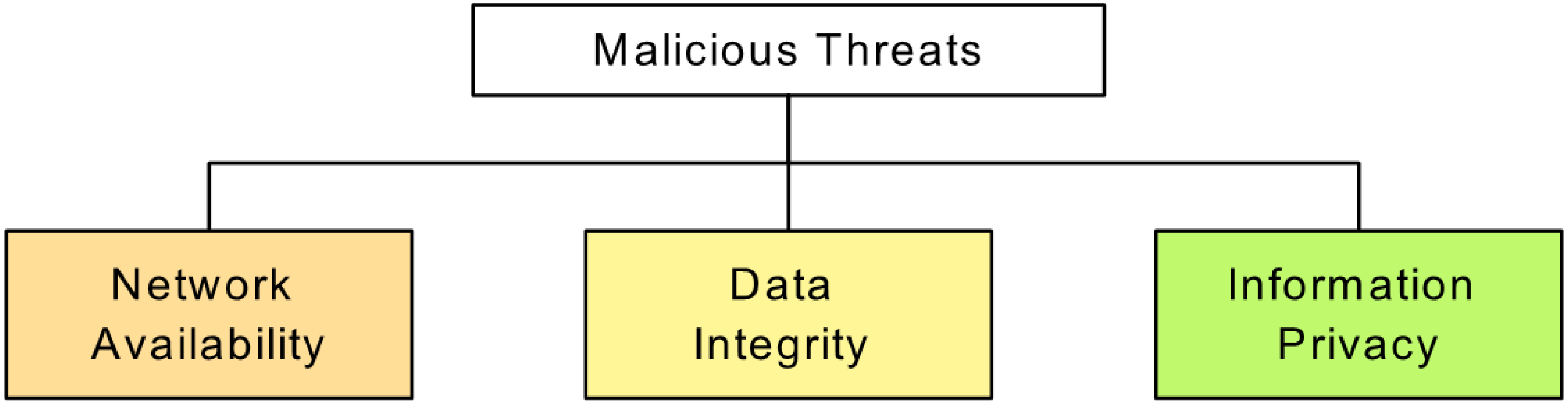
- **Various communication technologies: Fiber, Ethernet, WiFi, ZigBee, 3G, WiMax.**

# Smart Grid Network versus Internet

| | Smart Grid Communication Network | The Internet |
|---|---|---|
| Major Performance Metric | delay | throughput |
| Traffic Models | Periodic, constant | Power-law (WWW) |
| Communication Patterns | Bottom-up, top-down | End-to-end, peer-to-peer |

# Network Security Threats

- Security threats in conventional networks
  - Selfish behavior -> fairness
  - Malicious behavior -> network operation
- Security threats in the smart grid
  - Malicious behavior



# Attacks Targeting Network Availability

- Attempt to delay, block or corrupt information transmission to make network resources unavailable in the smart grid.
- Examples of potential attacks
  - Conventional DoS attacks: traffic-flooding, TCP sync attacks.
  - Wireless jamming. (Strasser'08, Popper'09)
- Differing from conventional networks.
  - Time-critical nature of traffic.
    - 3-ms delay threshold in power substation in IEC61850.

# Attacks Targeting Data Integrity

- less brute-force yet more sophisticated
- deliberately modify information to corrupt data exchange in this smart grid.

- Example:
  - False-data injection attacks (Liu’09).

- Authentication in the smart grid
  - Time-critical traffic. (3 ms, 10 ms) (Wang’09)
  - Short information length. (e.g., 20 bytes in a packet)
  - Key management

# Attacks Targeting Information Privacy

- **Attempt to eavesdrop on communications to acquire desired information.**
- **Examples:**
  - **Wiretapper.**
  - **Traffic analyzer.**
- **From the perspective of network operation, it has negligible effect.**
  - **The NIST smart grid report provides the priorities of the three security objective: (NIST Special Publication 1108).**
    - **Network availability**
    - **Data integrity**
    - **Information privacy**

# Outline

- Background and Motivation
- A glance of the smart grid and security
- A case study for traffic-flooding attacks.
  - A mini-showcase of the smart grid network
  - Delay performance measurement
- Conclusion

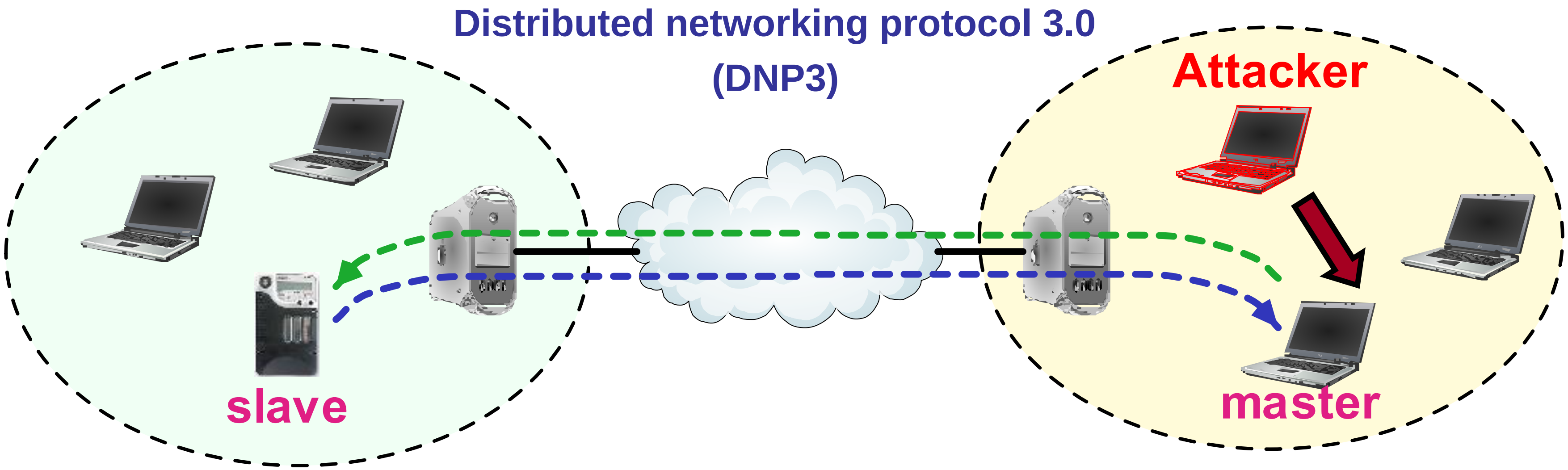
# Experimental Power Network

- Experimental power network in the FREEDM center at NC State university

- Backbone network:
  - Campus backbone network at NC State University

- Power substation networks:
  - Intelligent electronic devices (IED)
  - Intelligent fault management devices (IFM)
  - Interfaces:
    - Ethernet, WiFi, ZigBee

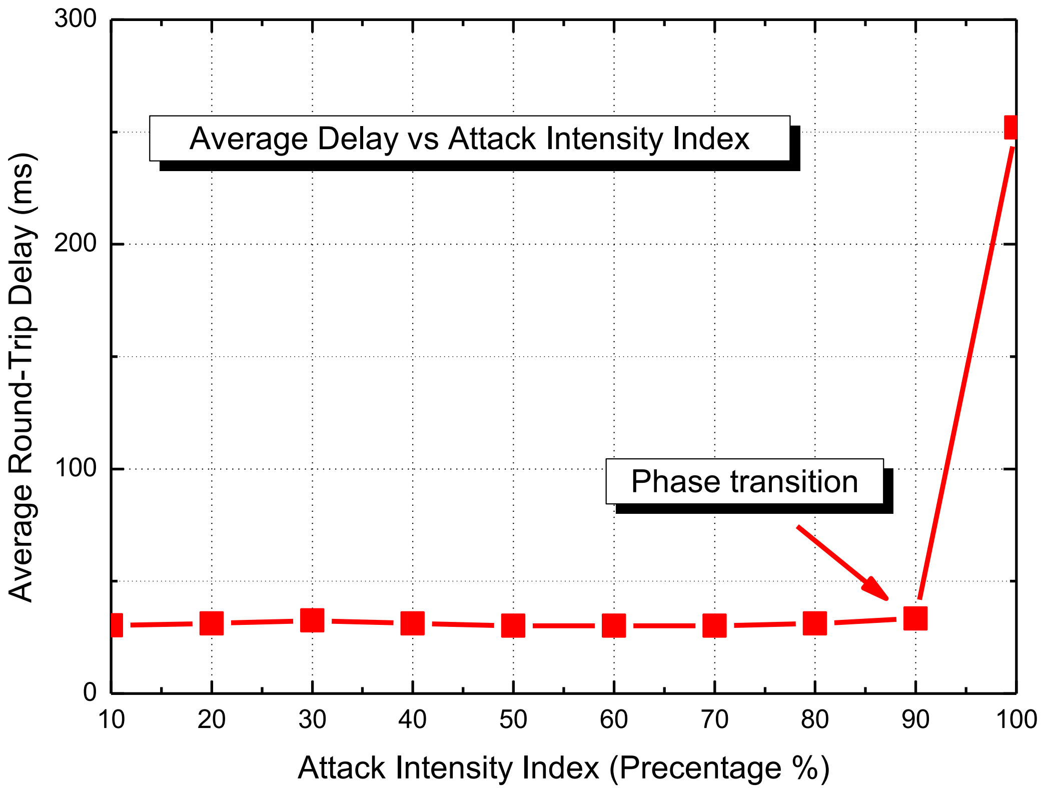
# Case Study: Traffic-flooding Attack



- **Why traffic-flooding attack?**
  - A type of denial-of-service attacks. (Adkins'03, Yu'08)
  - The one of the most easy-to-be-generated attacks
  - Attack intensity index:
    - I = rate of flooded traffic / channel bandwidth.
- **Performance metric:**
  - round-trip packet delay.

# Experimental Results (I)

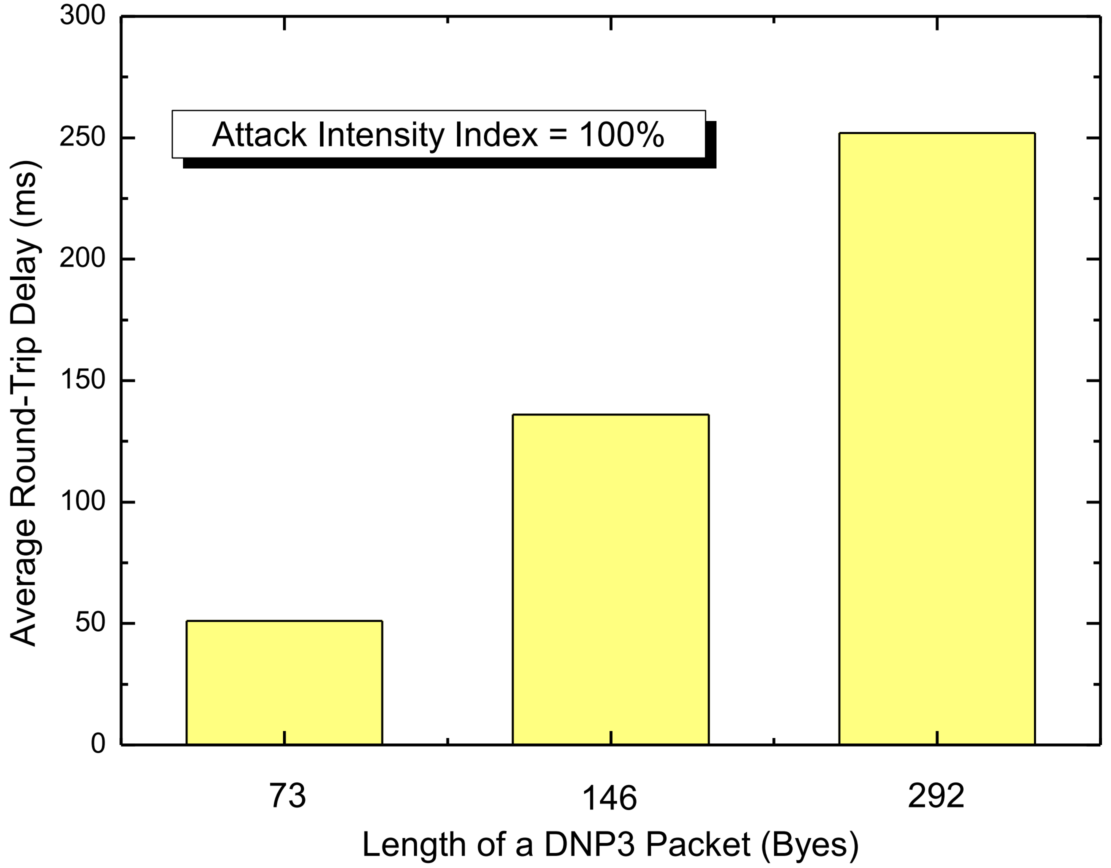
- **DNP3 packets are transmitted every 500 ms.**
  - **Very light traffic**



- **For light traffic, performance is significantly degraded when the attack intensity index approaches 1.**

# Experimental Results (II)

- **DNP3 packets are transmitted every 500 ms.**



- **Short DNP3 packets are more resistant to traffic-flooding attacks.**

# Outline

- Background and Motivation
- A glance of the smart grid and security
- A case study for traffic-flooding attacks.
- Conclusion

# Conclusion

- In this paper, we took a quick glance at security threats towards the communication networks in the smart grid.
- We used a case study to illustrate the impact of traffic-flooding attacks on a DNP3-based power system.
  - For light traffic in power networks, traffic flooding attacks only affect the delay performance when the attack intensity approaches 1.
  - Longer packets are more vulnerable to attacks.
- In-depth study via both analytical modeling and experiments is our future work.

# Thanks!