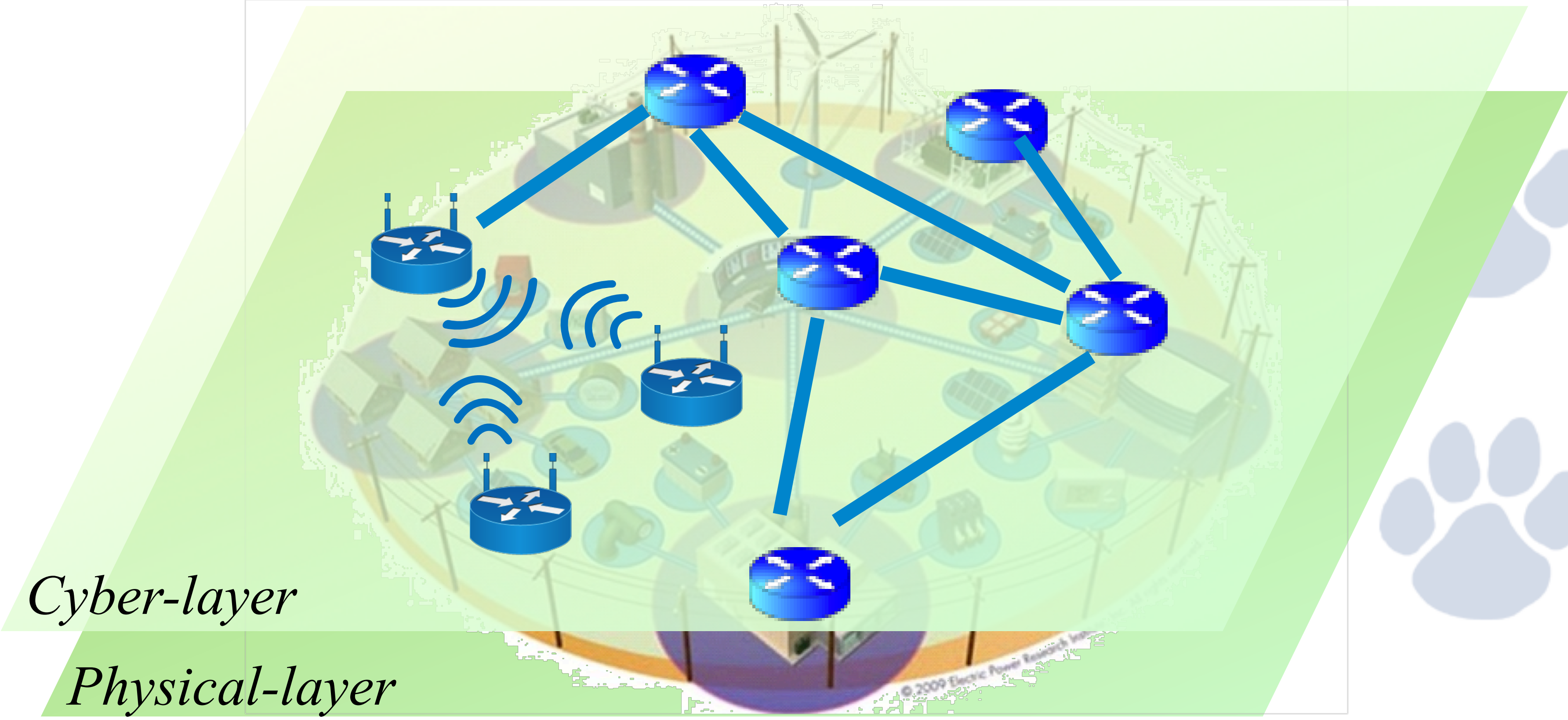
M2M Security in Smart Grid

Zhuo Lu, Assistant Professor
University of Memphis

M2M Communication in Smart Grid

- Smart Grid: next-generation power system
  - a large-scale cyber-physical system
  - networked control between machines



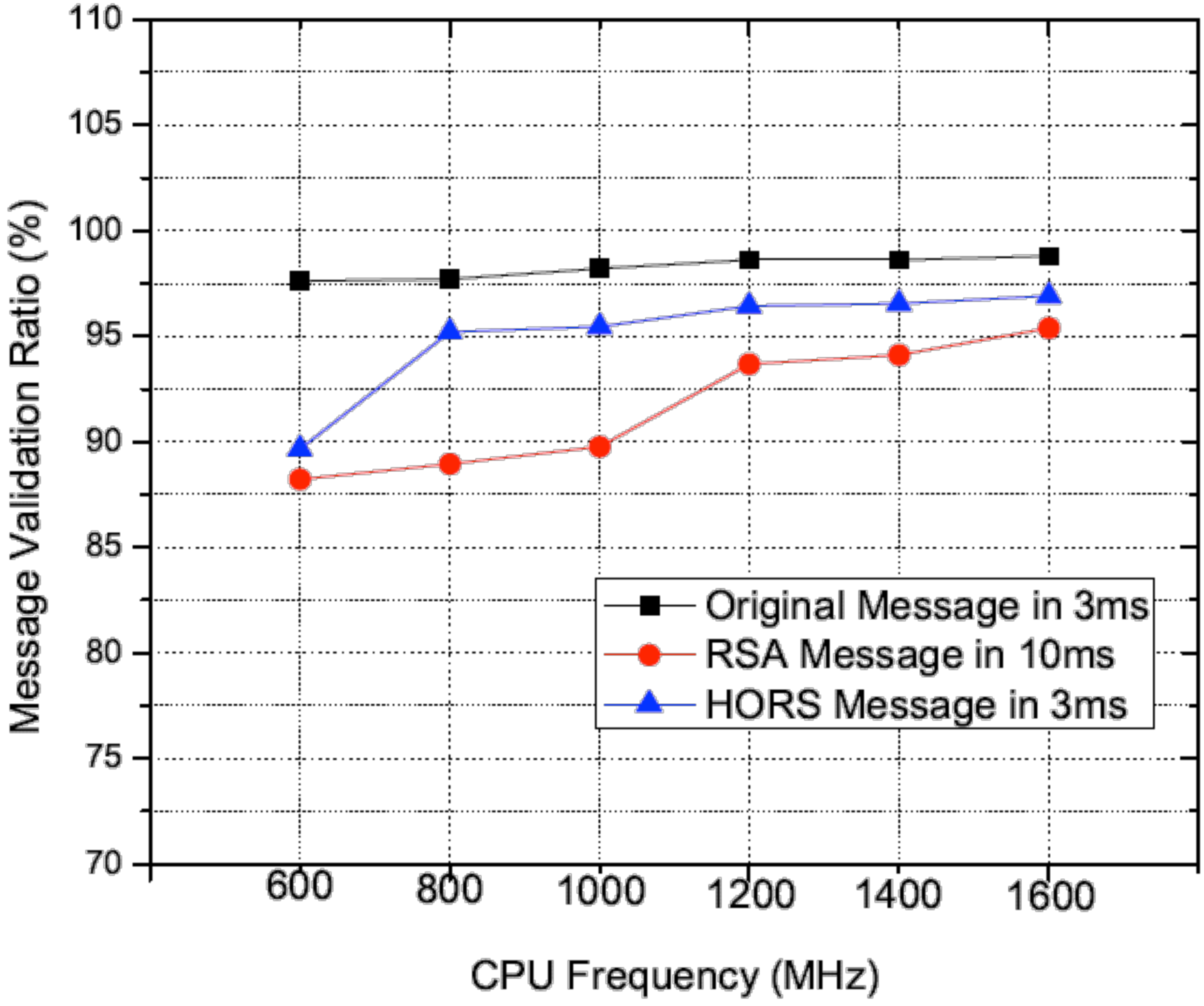
Challenge: Security vs Cost

- Different domains in smart grid
- Example: transmission and distribution domain
  - Communication-enabled control between devices
  - Message authentication is critical
  - Devices are using embedded computers
    - Typical CPU speed: a few hundred MHz
    - Cost is a big issue for both manufacturers and customers.

M2M Authentication in Transmission / Distribution Domain

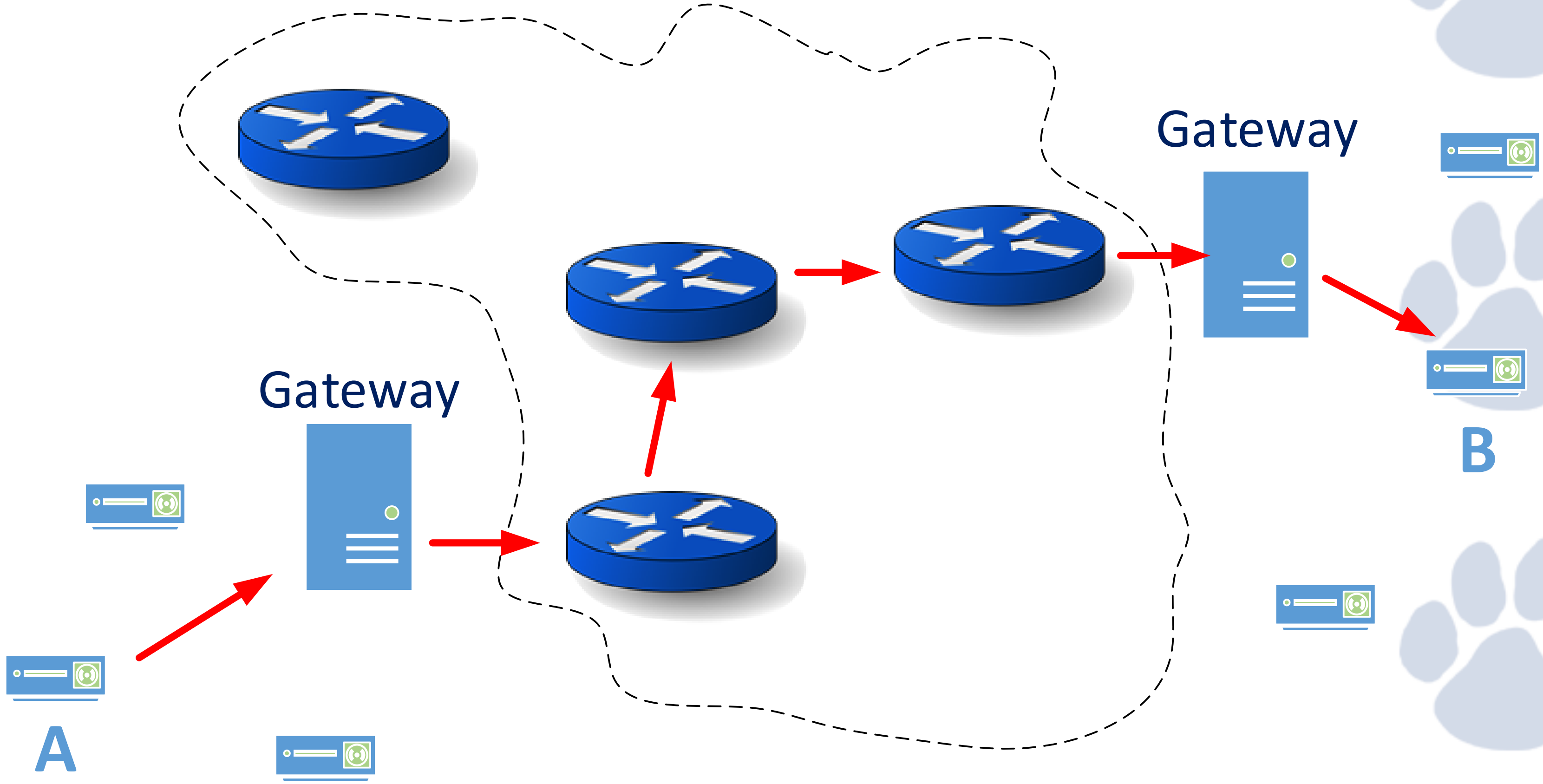
- Authentication schemes for control devices
  - Direct cost: delay performance
  - Indirect cost: Money
- Test: RSA vs Hash to Obtain Random Subsets (HORS)
  - Secure the GOOSE communication protocol in IEC 61850
    - Time-critical with timing requirements 3-10ms.
    - For protection control.

RSA vs HORS in M2M Communication



Security across Large Areas

- End-to-end security vs hierarchical security



Conclusions

- Smart grid features appealing applications of M2M communication and networking
- Fine grained security required in different domains
  - Security vs communication performance vs cost
- M2M in smart grid
  - Heterogeneous capabilities
  - End-to-end security vs hierarchical security