(POSTER) An Empirical Comparative Measurement on Real ICS Network Traffic to Internet Traffic

Chanwoo Bae, Won-Seok Hwang

National Security Research Institute (NSRI)

Motivation

- **Cyber-Physical Systems** = **Industrial Control Systems (ICS)**
  + Software & Network Systems
- ICS : machines, physical operations are driving (not human)
- Network traffic, any characteristic?
- We may guess but no proper measurement! Let's measure!

Data Collection

- Domain-scale networks
  - Campus vs ICS
  - Not Global-scale such as BGP

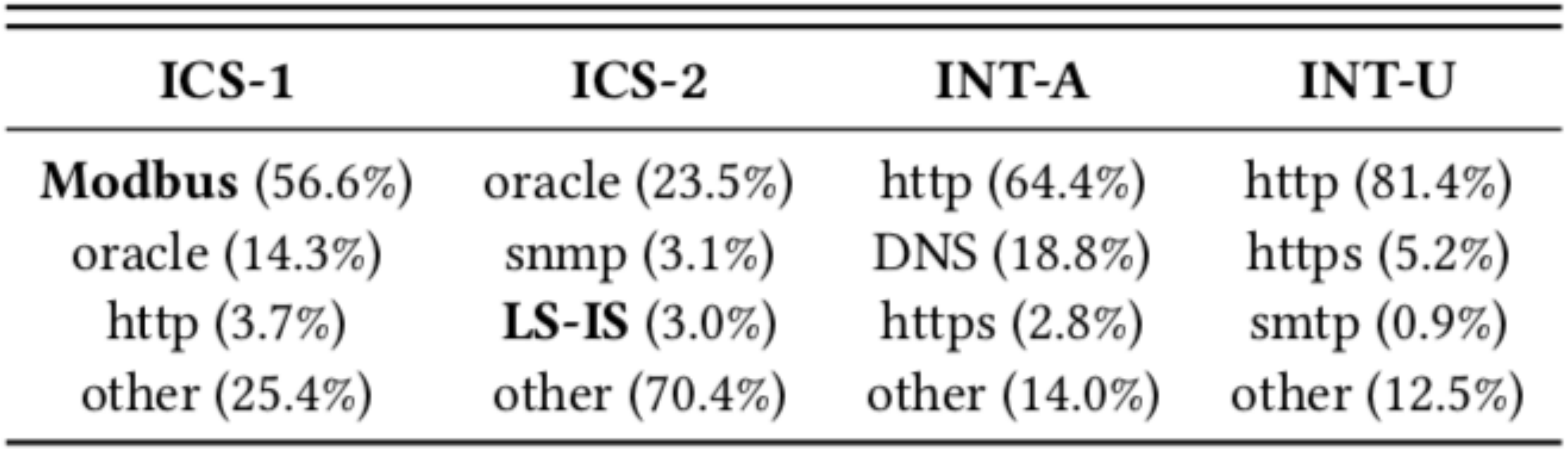
- ICS Network Traffic
  - Two Water Treatment Facilities (let's say **ICS-I, ICS-II**)
  - real-world sites in South Korea

- Public Internet Traffic (Campus Networks)
  - Auckland Univ. (wand.net.nz, lets say **INT-A**)
  - Wisconsin (pages.cs.wisc.edu/~tbenson/, lets say **INT-U**)

Traffic Utilization

- ICS traffic
  - Carrying control messages + oracle DB
  - machines generate traffic

- Internet traffic
  - HTTP + HTTPS + DNS are most

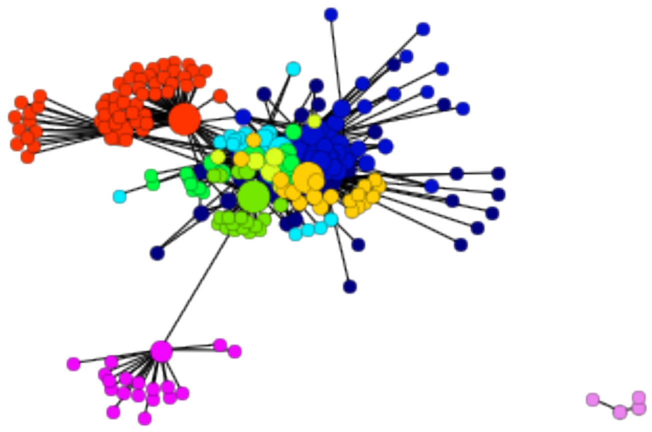


ICS-1	**ICS-2**	**INT-A**	**INT-U**
Modbus (56.6%)	oracle (23.5%)	http (64.4%)	http (81.4%)
oracle (14.3%)	snmp (3.1%)	DNS (18.8%)	https (5.2%)
http (3.7%)	**LS-IS** (3.0%)	https (2.8%)	smtp (0.9%)
other (25.4%)	other (70.4%)	other (14.0%)	other (12.5%)

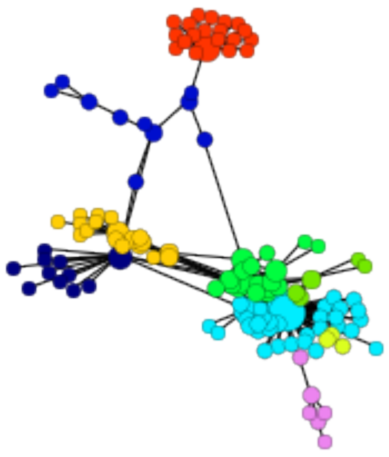
*** Modbus, LS-IS : Control Protocols for PLC**

Network Graph Analysis

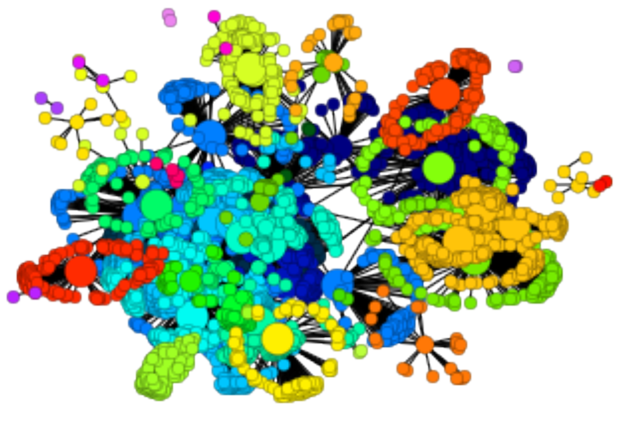
- Build Graph From the network traffic
  - aka., Traffic Dispersion Graph [1]
  - Nodes = distinct IPs
  - Edges = at least one packet



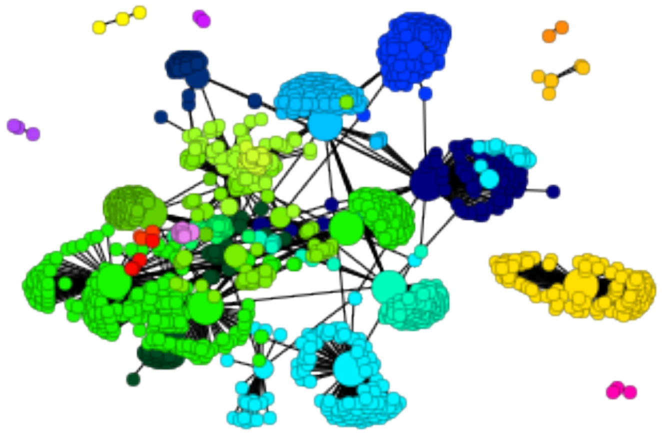
ICS-I



ICS-II



INT-A



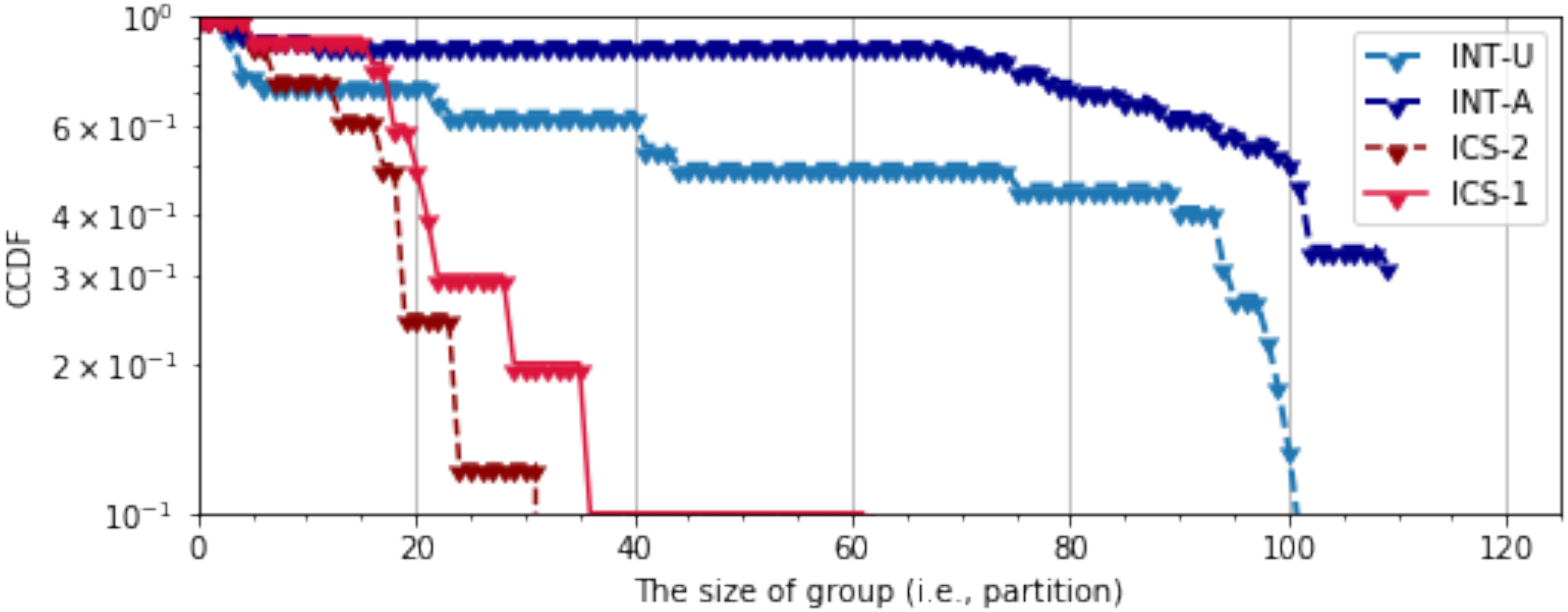
INT-U

[1] M. Iliofotou et al, Network Monitoring using Traffic Dispersion Graphs (TDG), Sigcomm 07

Network Graph Analysis

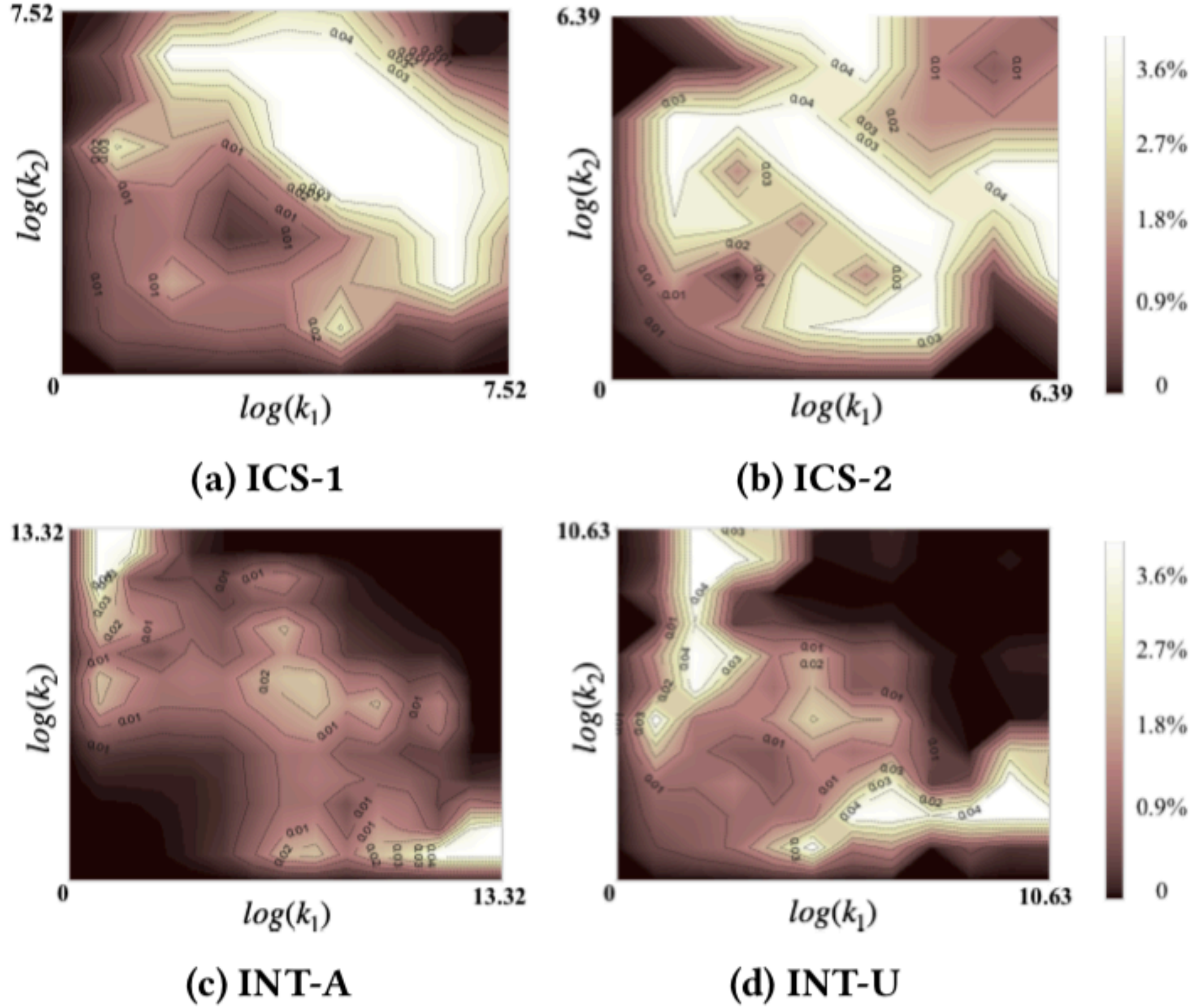
- Community size distribution
  - Using community discovery algorithm
  - Good to know group activity pattern

- Results
  - ICS traffic : relatively small size of group (20~40)
  - Internet traffic : massive size of group (~100)



Network Graph Analysis

- Joint Degree Distributions
  - Brightness in (x,y) : how many edges connecting degree x node and degree y node



(a) ICS-1

(b) ICS-2

(c) INT-A

(d) INT-U

- ICS Traffic
  - clustered by evenly distributed communities
  - p2p networks in each community

- Internet Traffic
  - right upper, left bottom areas
  - few selected nodes dominate most edges (famous sites)

Time-Series Analysis

- Time-Series Analysis
  - How Dynamic? 0-N Edges, Jaccard Index [2]
  - How Periodic? Autocorrelation Method
  - Detail score : refer the paper

- Results
  - ICS traffic is less dynamic than Internet traffic
    (maybe repeatedly operate same logic)
  - All flows are not periodic in ICS traffic,
    but flows of industrial protocols are relatively periodic

[2] M. Iliofotou et al, Exploiting dynamicity in graph-based traffic analysis, CoNEXT 09

Thanks

- **Source code for this paper is available at** cwb.kr:8080

- **We are happy to open anomaly dataset from an ICS**
  - Search “HAI Dataset” on Google

- **You can freely send me any questions to me !!**
  - cwbae@nsr.re.kr