# CNS Core: Small: Enabling Privacy-Preserving Routing-on-Context in IoT

PI: Tao Shu, Auburn University

Project website https://eng.auburn.edu/users/tzs0058/nsf_cns_2006998.htm

## Objectives

- Develop privacy-preserving context-driven routing mechanisms for IoT application over public Internet infrastructures
- Enable privacy-preserving context-aware computing for IoT
- Performance evaluation and validation based on simulation and testbed

## Challenges

- Over the past 50 years, Internet has evolved from initially a data network that was designed to connect only computers to a global-scale cyber-physical network that connects not only computers but also things in the physical world, coined Internet of Things (IoT).
- Surprisingly, the principle model of Internet routing has little change than what it was 50 years ago: largely defined by connectivity between nodes that is independent from application context.
- IoT traffic do not perform well under this traditional routing model, because these applications are typically closely coupled with the physical world and hence are context-oriented.
- As such, the overarching goal of this project is to establish a new routing primitive that supports efficient IoT routing based on the targeted application context, rather than on context-independent node connectivity.
- Due to the sensitive nature of the context information in many IoT application, "secure-by-design" privacy preservation is an intrinsic feature of our new routing mechanism.
- We also study privacy-preserving context-aware computing in IoT.


Fig. 1 Efficiency-privacy tradeoff in conventional geographic routing and goal of this research

## Scientific Impacts

- Create better understanding on the security and privacy vulnerabilities of IoT
- Renovate Internet routing paradigm by creating “secure-by-design” context-oriented routing for IoT traffic
- Enable privacy-preserving context-aware computing in IoT

## Solutions and Accomplishments

### Work 1: Space-encryption Routing

Method: Hilbert space filling curve for space encryption

- Space encryption: coordinate → HC index
- One-way transformation (privacy)

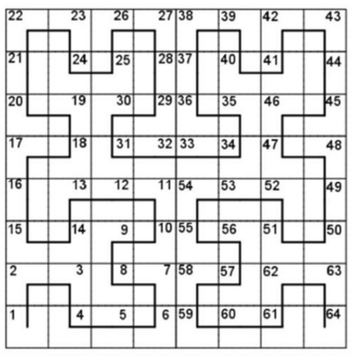


Fig. 2 a 2D Hilbert space filling curve and HC index

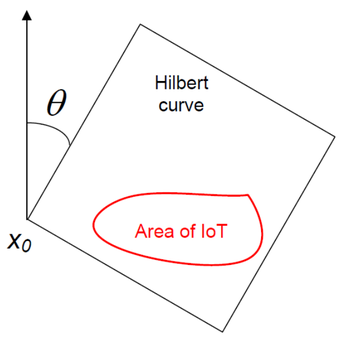



Fig. 3 One-way HC space encryption for an IoT network

Major accomplishments:

- For honest-but-curious insider attackers: a Kademlia-tree based hierarchical HC routing primitive to achieve efficient and privacy-preserving geographic routing
- For malicious outsider attackers: Rand-mix to achieve stronger communication privacy

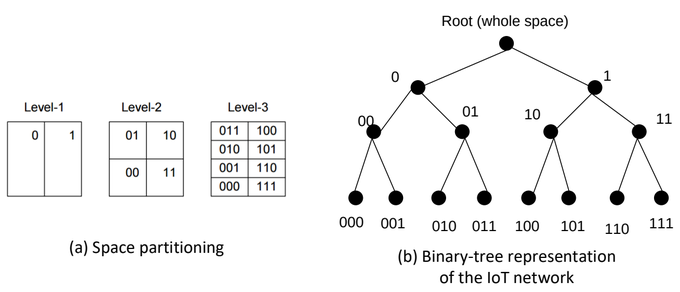



Fig. 4 Kademlia-tree based routing

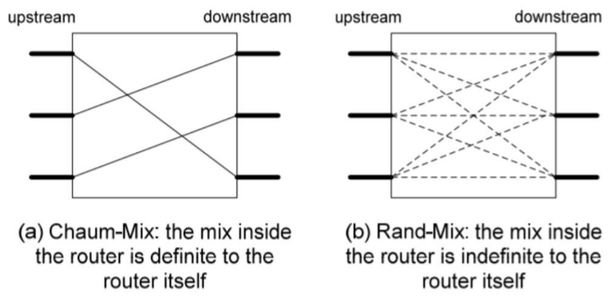
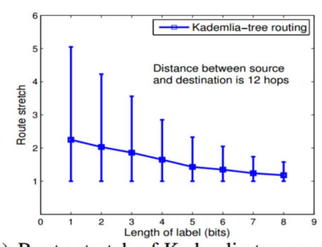


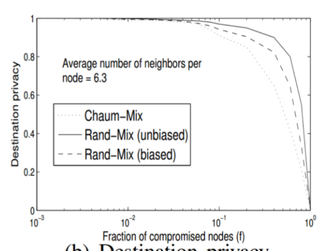

Fig. 5 Rand-Mix vs. Chaum-Mix. In Chaum-mix a router actually knows the true location of the next hop he is forwarding to, wheras in Rand-Mix the router itself doesn’t even know the true location of the next hop, because the address is just a 1D index.

Performance evaluation:




(a) Route stretch of Kademlia-tree routing

Observations: (1) Kademlia-tree routing not only reduces the mean route stretch but also the variance of the stretch
(2) The longer the label, the more efficient the route is




(b) Destination privacy

Rand-mix provides stronger privacy (in terms of entropy) than conventional traffic mix method such as Chaum-mix

### Work 2: Global Distribution Inference Assisted Backdoor Attack

Major findings:

- A malicious attacker can infer global data distribution in Federated Learning (FL) from global model update
- Global distribution inference can be exploited to launch early-stage backdoor injection that has higher attack success rate

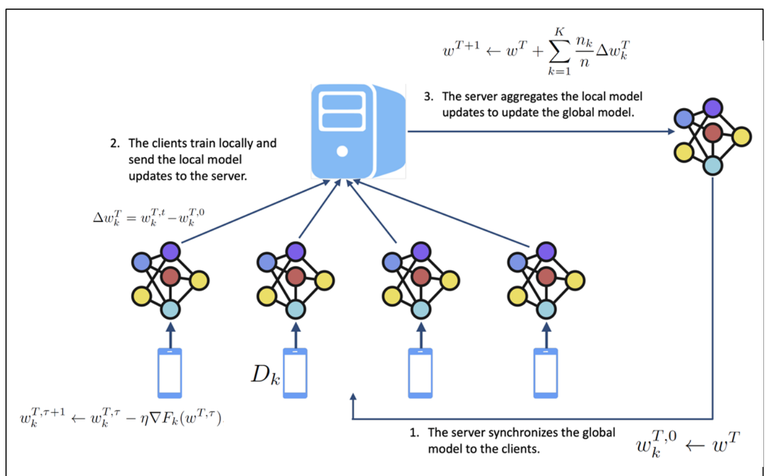
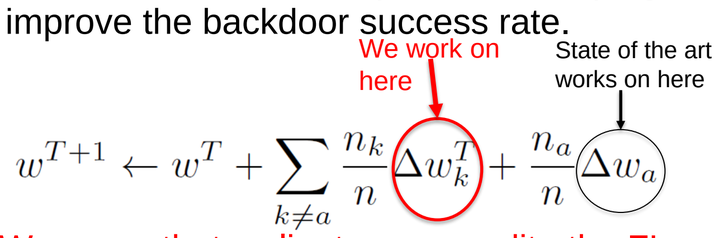



Fig. 6 FedAvg FL model

Major novelty: While the state of the art backdoor attack methods focus on directly optimizing the malicious local model, our approach manipulates the local model updates from “benign” clients to expedite global model convergence, and hence reducing the dilution to the effect of the malicious local model update and helping to improve the backdoor success rate.




We prove that a client can expedite the FL convergence by mimicking the distribution and gradients of a centralized learning on global data!

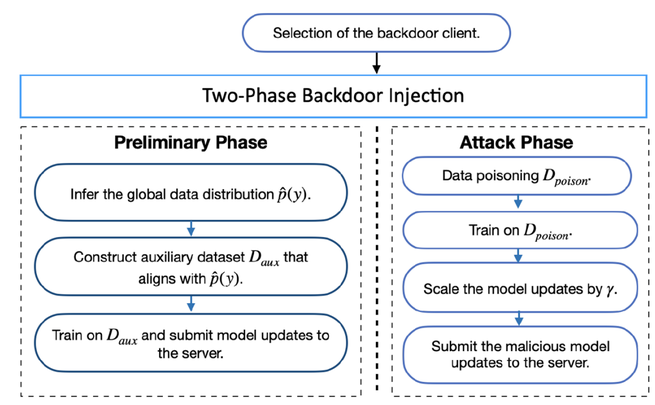
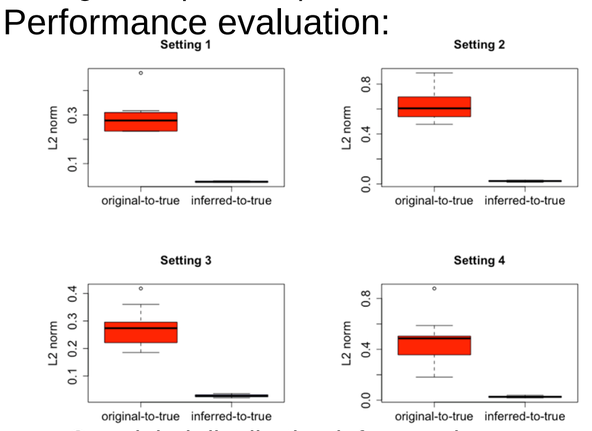
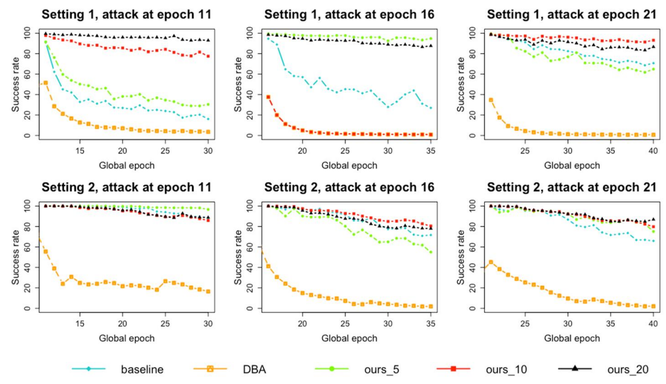



Fig. 7 Proposed 2-phase backdoor attack

Performance evaluation:




Our global distribution inference is accurate




Backdoor success rate is significantly improved by our method

## Broader Impact & Participation

- Bring privacy protection to millions of IoT users
- “Secure-by-design” context-driven routing that better fits into tomorrow’s IoT industry
- Outreach to under-represented groups
- New curriculum development, recruitment and training of graduate students