PERMIT: Privacy-Enabled Resource Management for IoT Networks

Anand D. Sarwate, Narayan B. Mandayam, *Rutgers University*

Sijie Xiong: Graduate Researcher

Motivating issues:

- IoT network devices have unique traffic "signatures."
- Very easy to do event-level detection using packet size and timing information.
- Future deployments may use gateways/coordinators to manage traffic.

Motivating issues:

- Can the gateway help to mask events?
- How can we use *differential privacy* to inform the design and management of future systems?
- How do we jointly manage privacy and network QoS?

Privacy framework:

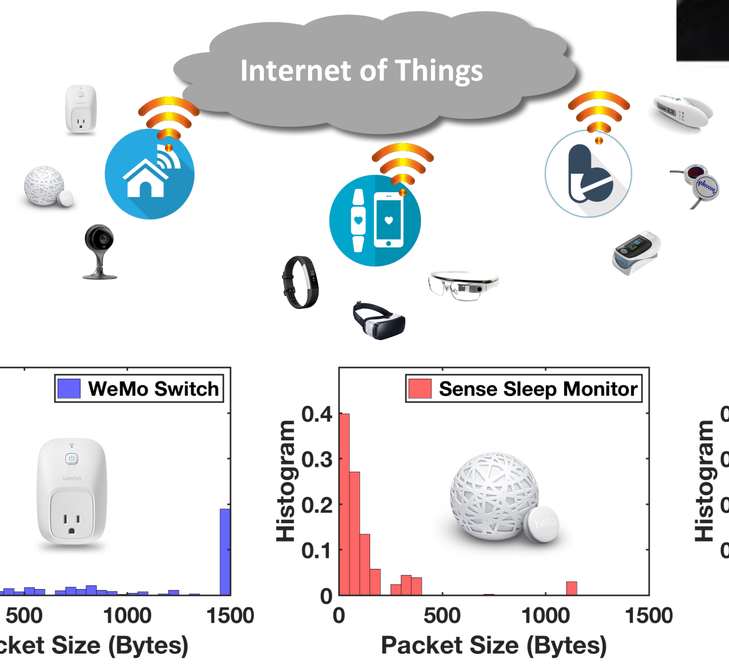
- Differential privacy uses random perturbations to mask the difference between *neighboring* ground-truth network traffic realizations.

Differential Privacy

An algorithm $\mathcal{A}(\mathbb{B})$ taking values in a set $\mathbb{T}$ provides (ϵ, δ)-differential privacy if

$$\Pr(\mathcal{A}(\mathbb{D}) \in \mathbb{S}) \leq \exp(\epsilon)\Pr(\mathcal{A}(\mathbb{D}') \in \mathbb{S}) + \delta,$$

for all measurable $\mathbb{S} \subseteq \mathbb{T}$ and all data sets $\mathbb{D}$ and $\mathbb{D}'$ differing in a single entry.



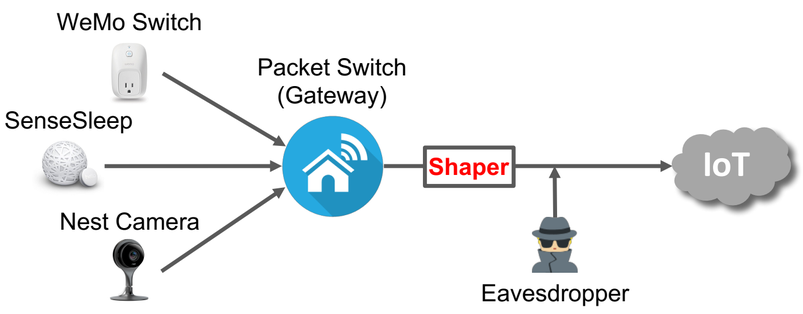
Main approach and contribution:

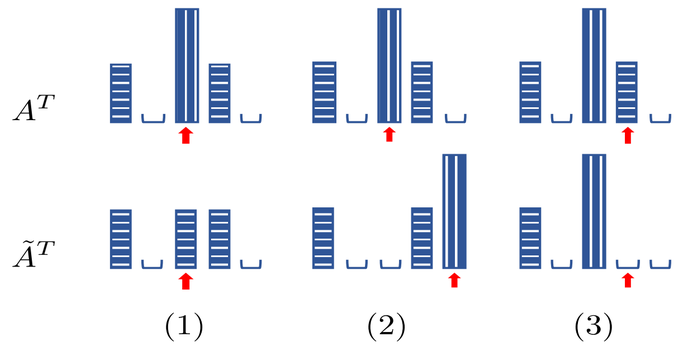
- Use a definition of discrete-time event-level neighboring streams for use with differential privacy.
- Develop a *traffic shaper* at the gateway using packet slicing and padding to obfuscate output packet stream.

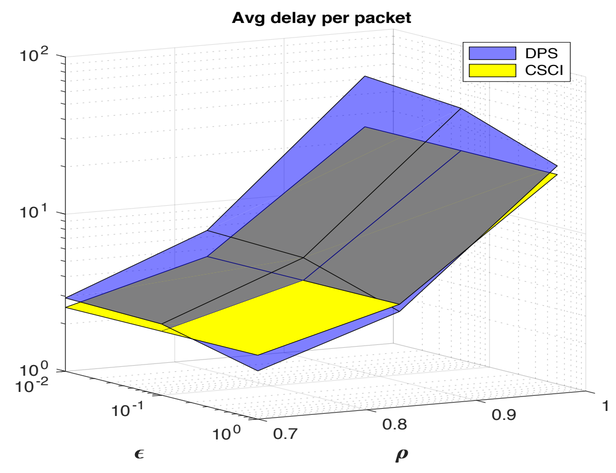
Constant Size Constant Interval	*Variable Size Constant Interval*
Constant Size Variable Interval	**Variable Size Variable Interval**

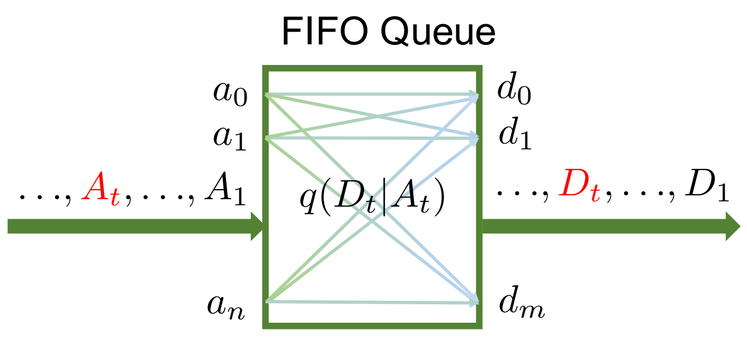
Case Study in Smart Homes:

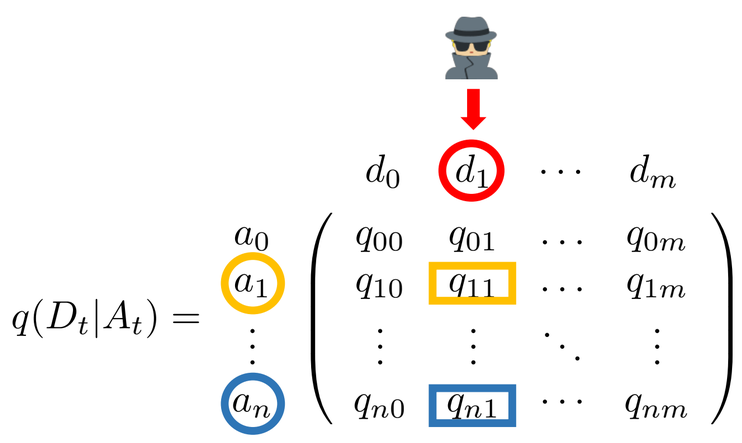
- Packet sizes and timing reveal private user activities.
- Privacy models on event-level adjacent streams.
- Differentially-private shaper vs. deterministic shaper.











Broader Impacts:

- Training graduate students in communications to work on privacy.
- Developing short course on differential privacy for non-CS audiences.
- Pursuing potential applications in wireless edge networks and hardware-based obfuscation mechanisms.

Publications:

S. Xiong, A.D. Sarwate, N.B. Mandayam, Privacy-Preserving Network Traffic Shaping Against IoT Side-Channel Leakage, *manuscript in preparation.*

K. Nikolakakis, D. Kalogerias, A.D. Sarwate, Learning Tree Structures from Noisy Data, in Proceedings of the Twenty-Second International Conference on Artificial Intelligence and Statistics (AISTATS), Ed. K. Chaudhuri, R. Salakhutdinov Vol. 89, pp. 1771–1782, 16–18 April 2019.

D. Bittner, A.D. Sarwate, R. Wright, Using Noisy Binary Search for Differentially Private Anomaly Detection, in Proceedings of the 2nd International Symposium on Cyber Security Cryptography and Machine Learning (CSCML), Ed. I. Dinur, S. Dolev, S. Lodha Vol. 10879, pp. 20–37, June 2018.

S. Xiong, A.D. Sarwate, N.B. Mandayam, Defending Against Packet-Size Side-Channel Attacks in IoT Networks, Proceedings of the 43rd IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Calgary, AB, Canada, pp. 2027–2031, 15–20 April 2018.

S. Xiong, A.D. Sarwate, N.B. Mandayam, Randomized Requantization with Local Differential Privacy, Proceedings of the 2016 International Conference on Acoustics, Speech and Signal Processing (ICASSP), Shanghai, China, pp. 2189–2193, 20–25 March 2016.