**Lumos: Identifying and Localizing Diverse Hidden IoT Devices in an Unfamiliar Environment**

The paper's authors are trying to solve a significant problem faced by many people across the world. They are trying to identify and locate hidden devices such as cameras, microphones, speakers, and other devices in unfamiliar environments such as Airbnb and hotel rooms. It is also assumed that people are not carrying any specialized equipment which is the case with most people. “Lumos” is a system proposed by the authors that can identify devices with up to 95% accuracy and locate them with up to 1.5m error, tested across 44 different IoT devices. Lumos consists of three modules - **1. Device fingerprinting Module**: This is a machine learning framework used to identify a diverse set of devices by analyzing the available packet header attributes. **2. Data collection module**: This is a model that learns the traffic pattern of each device over time to decide when and for how long to sense each wireless channel to identify devices across frequency ranges. **3. Localization module** is used to identify the location of hidden devices using signal strength and VIO traces.

**Strengths**:

* Lumos is compatible with Personal hand-held devices such as phones and laptops. This makes it extremely scalable and easy to use. No special hardware/equipment is necessary.
* Lumos can identify a diverse set of devices and localize up to 1.5m accuracy which is not possible with previous solutions such as bug finder, and camera detector.
* The end-to-end solution is implemented and available on an iPhone and Macbook which are widely used across the United States. Lumos is also fairly robust across typical changes in device settings making it very easy and convenient to use.

**Weaknesses**:

* Lumos use MAC addresses, and signal strength to identify and localize devices. However, sophisticated adversaries can evade Lumos using MAC randomization and randomly changing transmit power.
* Lumos can identify unprofiled devices only if similar device types were seen in the training corpus. Considering only 44 devices were tested, it's hard to tell how the system responds to new and unprofiled devices. More testing is necessary to check feasibility in real-world scenarios.
* Lumos needs to sniff the apartment/room for 30 minutes before it can identify and locate devices. This is a significant amount of time and the device needs to be charged during the sniffing or has considerable battery capacity to complete it.