IoT Anomaly Detection Via Device Interaction Graph: Discussion

While the evaluation result shows that CausalIoT outperforms the existing work, we consider it the first step towards interaction-aware anomaly detection at smart homes. As a result, we list some limitations that we plan to address.

Unmeasured confounder. In Section VI, we highlight that some unmeasured factors (e.g., the sunrise) come from the environment. These factors result in spurious interactions, which eventually reduce the detection accuracy and interpretation capability. The best solution is collecting environmental information about smart homes (e.g., the weather). Since CausalIoT can be easily extended, we can introduce additional nodes that represent the environmental factors, and study their relationship with the device. By doing so, the generated device interaction graph will encode more fruitful information, and the inferred interactions among devices will be more accurate.

Stationary assumption. While TemporalPC achieves good detection accuracy, it is initiated in an offline way. The inferred device interaction graph only describes the interactions during the collection period, and the stationary assumption is needed for applying the graph to handle the runtime device event. As a result, it is susceptible to the scenario where the interaction graph changes. For example, there may be behavioral deviations, or users may add/remove a device. While CausalIoT can use a new training dataset collected within a short period and efficiently re-train the interaction graph, other alternatives are worth exploiting, e.g., runtime inference of the interaction graph.

Multi-user scenarios. Finally, our work focuses on the interaction graph construction in a single-user setting. However, when extending to the multi-user scenario, the graph construction can be complicated as different users may have different preferences about smart home usage. Even worse, some preferences may be conflicted (e.g., user A deploys an automation rule "Turn on the light when the TV is on", while user B deploys a conflicted rule "Turn off the light when the TV is on"). Some auxiliary information (e.g., temporal information) may help to distinguish the device usage for different users and assist in the interaction mining for each user.