Policy Management for Internet of Things

Mentor: Shan Lin
Bryan Hallock, Anthony Brangaitis

Stony Brook University
Electrical and Computer Engineering

Abstract:

As IoT devices are currently developed independently of one another, and as consumers begin to desire more interoperable devices, policy differences can arise within IoT systems. As manufacturers begin to allow their devices to interact with those outside their device ecosystem, the problems caused by these policy differences will begin to embolden, unless an overarching policy management system is developed and agreed upon. In this project we look at how IoT systems are designed and operate in the real world, explain how policy differences can occur, and categorize these policy differences to better understand how to handle them. We then give an idea of what an ideal solution would do, review commonly proposed solutions, and discuss the strengths and shortcomings of these solutions. Finally we discuss simulations and visualizations of these systems.

Common Terms:

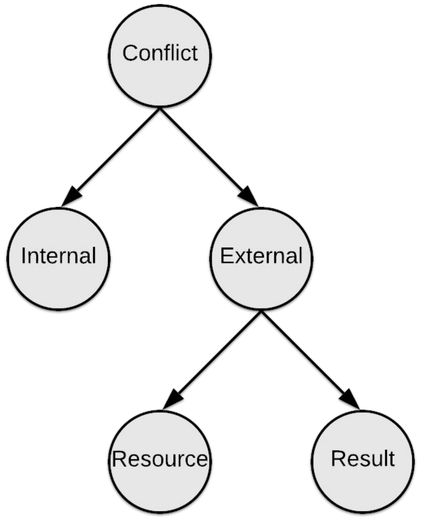
IoT - Internet of Things, the set of everyday objects with an embedded computing device which has allowed them to connect to the internet to send and recieve data

Resource/Actuator - IoT devices that typically can only receive data from other devices, which guides their operation

Conflict - multiple IoT devices attempt control of the same resource or environment state

Conflict Categorization:

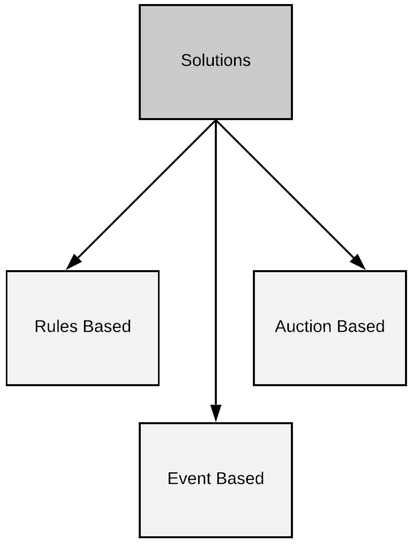
We defined conflicts into **internal** and **external** conflicts. An internal conflict is a case where within one device ecosystem (such as Amazon's Echo product line), there is an internal issue in the policies guiding operation. We chose to define this category to acknowledge the issues we found in our device observations. External conflict are the issues in policy management that are presented by the lack of interoperability between manufacturers. We further divided external conflicts into **resource** and **results** conflicts. A resource conflict denotes a case where multiple devices attempt control over the same resource. Typically, they may prevent one another from doing so and potentially freeze operation of the system, which in a real time system is not acceptable. A results conflict is when multiple devices in a system launch protocols which attempt to modify the same environment state. In this case you have to determine which device should get priority and cancel the other request.



Solution Types:

We divided solutions to managing IoT systems into three categories:

- Rules Based
  - The system has a set of rules it has to follow
  - This set of rules generally has to be made beforehand
  - Rules grow exponentially as population of a system grows
- Event Based
  - The system reacts to changes in its environment
  - These reactions can be immediate
    - Systems can determine solutions to problems as they arise
  - Or these reactions can be predictive
    - Systems planning response to future predicted problems
- Auction Based
  - These systems use auctions to decide conflicts
  - The winner spends currency to win results
  - Fairness is determined by lack of funds



Many of the solutions researched were capable of handling a diverse population of task inherent to IoT systems. However, the trouble lies is development of an algorithm that handle the large and ever increasing population of IoT devices. This creates effective management of small scale systems but presents a tradeoff of exponentially increased processing times on the large scale.

Acknowledgements:

We would like to express our thanks to professors Shan Lin and Harbans Dhadwal for their guidance on this project.

BAX Inc