Jamming in the Internet of Things: A Game-Theoretic Perspective

Nima Namvar

North Carolina A&T State University

nnamvar@aggies.ncat.edu

December 7, 2016

Overview

1. Introduction
2. IoT security
   - Jamming attack
   - Problem Formulation
3. Proposed Algorithm
4. Simulation Results
5. Conclusions

Introduction

- The Internet of Things (IoT) is emerging as an attractive 5G network architecture that promotes billions of devices and services to interconnect and exchange useful information and data.
- IoT refers to a network of uniquely identifiable interconnected virtual and physical objects, such as sensors, radio frequency identification (RFID) tags, actuators, and mobile phones which are able to communicate and exchange data with each other to perform different tasks

Introduction

IoT enabling technologies:

- Wireless Sensor Networks (WSN)
- Cloud computing
- Big data analytics
- Embedded systems
- Communication protocols
- Web services
- Mobile internet

Introduction

IoT poses a bright foreground for the formation of smart environments and self-conscious and autonomous devices. Some applications of IoT are:

- Home automation: smart lighting, smart appliances
- Medical aids: health monitoring, wearable electronics
- Cities: smart parking
- Environment: weather monitoring
- Energy: smart grids
- Industry: machine diagnosis

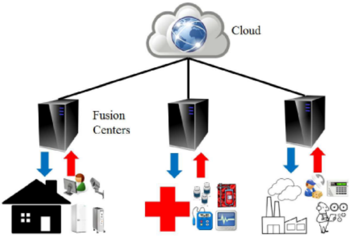

Fig. 1. Fusion centers acting as designated data aggregation hubs and access gateways to the cloud for personal, hospital, and industrial environments.

Security of IoT

Due to its large attack surface, the security of an IoT system is prone to a variety of attacks such as:

- Malicious radio jamming
- Denial of service (DoS)
- Side channel attack (SCA)
- Replay attack
- Node capture

In the absence of solid security in place, attacks and malfunctions in the IoT may outweigh any of its benefits.

Jamming attack

Jamming attack makes the battery of target devices to drain quickly by disrupting their data transmission and making them retransmit repeatedly. Moreover, jamming could also lead to Denial of Service.

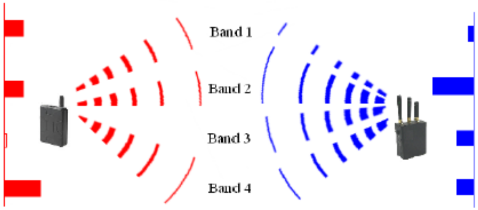

Figure: A Multitone Jammer $\mathcal{J}$

Modeling the jamming attack: Assumptions

Consider an OFDM-based IoT network consisting of an access point (AP)and M IoT devices. $\mathcal{S} = \{s_1, s_2, ..., s_N\}$ denotes the set of N subcarriers which are allocated to the devices.

The IoT devices are operating on sub 1 GHz license-exempt bands and are connected to the AP under IEEE 802.11ah (low-power WiFi).

We consider a multi-tone jammer $\mathcal{J}$ which aims at disturbing the performance of IoT network by transmitting over some subcarriers (tones) to:

- Decrease the link SINR
- Increase the bit error rate (BER)

Modeling the jamming attack: Assumptions

The IoT controller, or AP, confronts the jamming attack by intelligently distributing its power over the subcarriers in such a way that protects as many IoT devices as possible from the jamming attack.

How to model the problem?

Modeling the jamming attack: Assumptions

The IoT controller, or AP, confronts the jamming attack by intelligently distributing its power over the subcarriers in such a way that protects as many IoT devices as possible from the jamming attack.

The question is, how the AP should distribute its power over the set of channels? How to model the problem?

Colonel Blotto games

The *Colonel Blotto* game is a fundamental model of strategic resource allocation in multiple dimensions, in which two players compete over a number of independent battlefields by distributing their forces over these battlefields and within each battlefield, the player that allocates the higher level of force wins.

Game components

- Colonel 1: IoT access point (AP)
- Colonel 2: The jammer $\mathcal{J}$
- Battlefields: $\mathcal{S} = \{s_1, s_2, ..., s_N\}$

Colonel Blotto model

Formally, the definition of Blotto game in our problem is:

Definition

The *Colonel Blotto* game which is labeled as $CB[AP, \mathcal{J}, \mathcal{S} = \{s_i\}_{i=1}^{N}]$ is the one-shot game in which players, namely AP and jammer ($\mathcal{J}$), compete by simultaneously announcing distribution of their power over the set of N subcarriers subject to their power budget constraints. Each battlefield, i.e. each subcarrier $s \in \mathcal{S}$, is won by AP if transmission over s, as a function of power allocation strategy by both players, is successful and is won by the jammer, otherwise. The payoff for the whole game is the proportion of the wins on the individual battlefields.

Payoff Functions

Subcarrier SINR

$$SINR_s^{sub} = \frac{H_s^{AP} p_s^{AP}}{N_0 + H_s^J p_s^J}, \forall s \in \mathcal{S} \tag{1}$$

Successful Transmission Condition

$$\frac{p_s^{AP}}{N_0 + p_s^J} \geq \tau \tag{2}$$

Payoff Functions

$$U_{AP}(p_s^{AP}, p_s^J) = \frac{1}{N} \sum_{d=1}^{N} \frac{1}{2}(1 + \mathrm{sgn}(\frac{p_s^{AP}}{N_0 + p_s^J} - \tau)) \tag{3}$$

$$U_{AP} + U_j = 0 \tag{4}$$

.

Possible Solutions of Blotto game

- Example:
  For the case of 3 battlefields and total of 6 troops on each side:
  - $(0,0,6)$ vs. $(1,2,3)$?
  - $(2,2,2)$ vs. $(1,1,4)$?
  - $(3,2,1)$ vs. $(1,1,4)$?

General solution

- A best strategy is NOT a pure strategy. It must be a mixed strategy.
- Obtaining the Nash equilibrium in mixed strategies for Blotto games with $N > 3$ fields and asymmetric resources has been an open problem since 1930.

Proposed Algorithm

Base on the ratio of available resources for the players, there are different sets of Nash equilibria. If $P^{AP} > NP^{J}$, the game has a set of trivial optimal strategies for AP, with $x_i^{AP} = \frac{P^{AP}}{N}$, for all $i = 1, 2, ..., N$.

We are particularly interested in the scenario of $P^{AP} < NP^{J}$ and $P^{J} < NP^{AP}$, for which there is no pure Nash equilibrium.

Proposed Algorithm

We propose an evolutionary learning based algorithm, which learn the best strategies by playing the game repeatedly. The algorithm converges to optimal solution, yet, there is no solid proof due to its nature of being evolutionary-based (similar to GA).

Proposed Algorithm

- We consider a population of size $K = K_{AP} + K_J$ of K_{AP} players of the type AP and K_J players of the type $\mathcal{J}$. Players of the same kind have identical resources; however, each player may adopt a different strategy profile.
- The Blotto game is played successively by randomly chosen pairs of opponents and, the players' strategies evolve in response to the resulting payoffs.
- In each round, each player may face an opponent of its own type or of the opposite type with probabilities ϵ and $1 - \epsilon$, respectively.

Proposed Algorithm

Adaptation is based on the average payoff:

Expected payoff in each round for AP players

$$\pi^i_{AP} = \frac{1}{K_J} \sum_{z=1}^{K_J} \int_0^{P^{AP}} \int_0^{P^J} U_{AP}(f_i(x,t), h_z(x',t))dxdx', \qquad (5)$$
$$\forall i \in \{1, 2, ..., K_{AP}\}$$

Expected payoff in each round for J players

$$\pi^i_{J} = \frac{1}{K_{AP}} \sum_{z=1}^{K_{AP}} \int_0^{P^{J}} \int_0^{P^{AP}} U_{J}(f_z(x,t), h_i(x',t))dxdx', \qquad (6)$$
$$\forall i \in \{1, 2, ..., K_{J}\}$$

Dynamic Evolution Rules

Imitation

At each time step, for each player j, another player j' of the same kind is randomly selected from the entire population and their average payoffs are compared. If $\pi_j < \pi_{j'}$, player j *imitates* player j' by adopting its strategy $f_{j'}(x)$, otherwise, the strategy of player j does not change.

Mutation

To increase the diversity of the strategy sets, we assume that the strategy of each player j is subject to a process of mutation with small probability ξ in which, an amount of $2u$ is subtracted from the strategy of j at a randomly selected point and the amount u is added to the two nearest points in the mixed strategy vector.

Result of the Proposed Algorithm

The proposed algorithm converges to mixed Nash Equilibrium, which is the optimal solution, and its performance can be compared with the literature.

Nash Equilibrium in mixed strategies

$$U_j(f_j(\underline{x})^*, f_{-j}(\underline{x})^*) \succeq U_j(f_j(\underline{x}), f_{-j}(\underline{x})^*),$$
$$\forall f_{AP}(\underline{x})^* \in \Pi_{AP}, f_J(\underline{x})^* \in \Pi_J, \tag{7}$$

Simulation Results

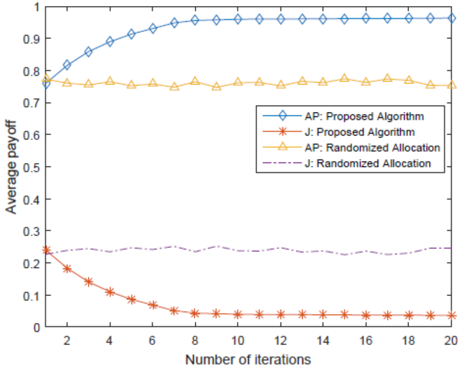

Fig. 2: The average payoff of $\mathcal{AP}$ and $\mathcal{J}$ according to the proposed algorithm and random allocation strategy.

Simulation Results

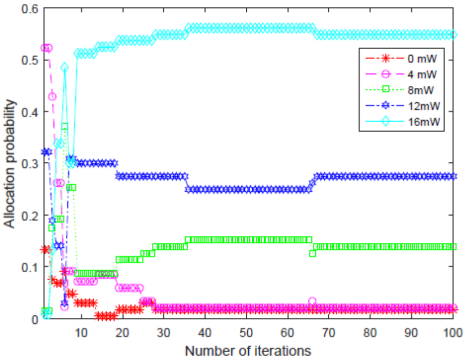

Fig. 3: The evolution of $\mathcal{AP}$'s mixed strategy. The power of $\mathcal{AP}$ for each subcarrier is discretized to $L = 5$ levels to show the convergence of the proposed algorithm.

Simulation Results

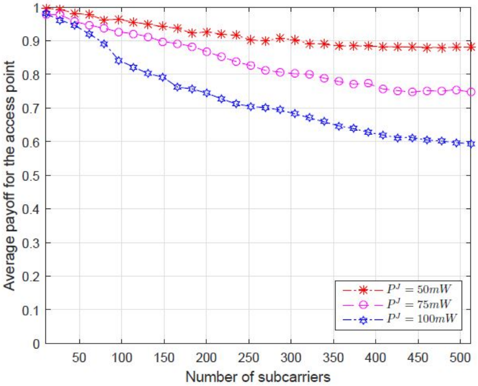

Fig. 4. Average defender's payoff for different network sizes.

Simulation Results

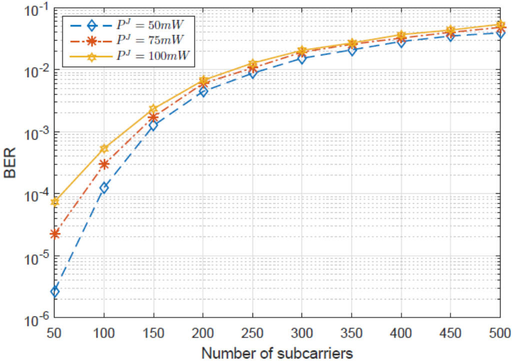

Fig. 5. Average BER for different network sizes.

Simulation Results

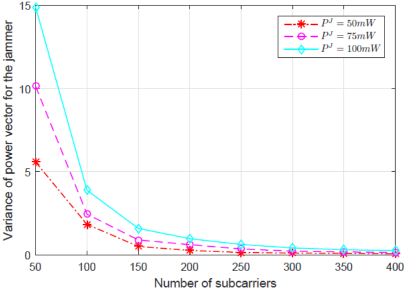

Fig. 6. Variance of the jammer's power allocation vector for different network sizes.

Conclusions

- In this paper, we have studied the problem of jamming in an IoT system.
- In particular, we have proposed a centralized mechanism to address the jamming problem in an IoT system composed of resource constrained devices.
- We have modeled the problem as a Colonel Blotto game between the IoT access point and the jammer. In this game, each player seeks to maximize its payoff by adopting a randomized strategy to allocate its power to the subcarriers.
- To solve this game, we have proposed a novel evolutionary-based algorithm to find the equilibrium strategies for both players.

THANK YOU!

- *Perhaps it is good to have a beautiful mind, but an even greater gift is to discover a beautiful heart.*

  -John Nash