1 Introduction

Game-theoretic ideas arise in many contexts. Often these settings are not called games, but they can be analyzed with the same tools. A decision-maker's outcome depends on the decisions made by others. This introduces a strategic element that game theory is designed to analyze. However, game-theoretic ideas are also relevant to settings where no one is overtly making decisions. We examine the behavior of agile and heterogenous nodes in a network environment, and model the evolution of the player type under different network conditions. Network security is a primary concern in open, dynamic and heterogeneous networks such as Internet and wireless mobile networks, which are prone to security risks, which have a detrimental effects on network performance. In this context, research efforts are directed towards:

- Characterizing the network model, incorporating constraints and underlying structure from well established quantative models.
- Characterizing malicious attacks incorporating the specific features of modern networks.
- Designing and refining (non)cooperative mechanisms.
- Designing and refining defense mechanisms.

Evolutionary biology provides an example. A basic principle is that mutations are more likely to succeed in a population when they improve the fitness of the organisms that carry the mutation. But often, this fitness cannot be assessed in isolation; rather, it depends on what all the other (nonmutant) organisms are doing and how the mutant's behavior interacts with the nonmutants' behaviors. In such situations, reasoning about the success or failure of the mutation involves game-theoretic definitions, and in fact very closely resembles the process of reasoning about decisions made by intelligent actors.

The utilization of game theory to study the network security problems has attracted considerable research and has led to valuable insight on the attackers' behaviour and the optimal strategy for the network defenders. A security game on a network is usually modeled by using a graph. We are motivated by modern network advances to model network security problems with perspective from a game theoretic analysis:

1. Game theory is a powerful tool to model the interactions of decision makers with mutually conflicting / complimentary objectives. e.g., the interaction between the attackers and the network defenders / heterogenous utility functions and competing / contended nodes.
2. Game theory (particularly non-cooperative game theory) can model the features or constraints of modern networks such as lack of coordination, network feedback and topology.

Game theory can serve as a validation tool to evaluate the proposed solutions. However, most of them are focused on the characterization of the Nash equilibrium (NE) of the formulated security game and the defenders' strategy at the NE, few of them performs a systematic study on the complexity (in terms of time and space) of how to solve the game and reach the NE from a foundational game theory perspective. The proposed study aims at filling this gap by establishing necessary theoretical foundations under the game algorithmic framework.

2 Related work

(Under construction...)

3 Proposed Topic

In order to construct a viable model for our final goal, we must have (1) self-configuration, and (2) automatic neighbor relations. We address our CRs as a finite set of actions, and formalize the game play as sphere-of- influence (SIG) graph. To begin, we propose a set of mixed strategies defined by a probability distribution over the finite set of feasible strategies, and define a basic game played by the cognitive nodes. Taking a queueing game, we have a basic set of strategies represented by a sampling of queues. This example is particularly useful in large, decentralized networks. The basic topology of the SIG graph under these rules allow for the projection of the decision process of the game into a higher-dimensional complex space. We analyze the interaction of the nodes as a topological graph, which we may then apply our statistical game theoretic approach. We do this by forming an arrangement. Given strategies s_1, s_2, and a function ϕ, we examine the expanded strategy space where s_1 stochastically dominating s_2 implies that $E[\phi(\cdot, s_1)] > E[\phi(\cdot, s_2)]$. This space is well-publicized in marketing theory, where valuation functions are often given as right-continuous, left-limited functions. As we expand the strategy space, new topologies emerge as a result of the SIG graph, allowing for the insertion of additional properties. We make use of mean field theorem, for which the study of arrangements is well-defined, to increase the complexity of the congnitive nodes' interaction space, and model it as a complex field topology. The decision model in the extended strategy space is modeled as an Ito drift diffusion process, allowing us to make use of the Poisson process and binomial theorem. We conjecture that the choice of arrangement and random process to be in this space results in additional immersions of the SIG graph with nice properties.

Continuing, we model the additive noise and determine the rate of random mutation given in the evolutionary model. We conjecture that in this setting, we will be able to examine the interactions of the cognitive nodes, and model the evolution of their types. Given the goals of quality-of-service and robustness to adversary (mutant) nodes, we will be able to realistically determine the outcome of the game based on the intelligence of the nodes.

4 Research Plan

As an initial plan, the project will consist of the following main steps, which are also the main milestones of establishing the pertinent game algorithmic foundation on the network security problems.

- Step 1: Study network security problems (literature study on the network security) and the relevant graph models. Formulate the network games using appropriate abstraction.
- Step 2: Establish the existence, uniqueness if the case, of the NE of the formulated security game. In case where the problem is NP complete, derive the relevant approximation or non-approximability results with distributed heuristic polynomial algorithms.
- Step 3: Study the programming of cognitive nodes, tensorflow.
- Step 4: Based on the analytical results, implement protocols and security solutions for various scenarios.

5 Plan for completion of research

The criteria to evaluate the obtained work are:
Theoretically, the success of the study is attested by the establishment of game algorithmic foundation of the network security problems and the relevant algorithms developed to solve the formulated

security game and reach the NE of the game.
Practically, the study is evaluated by the proposition of protocols and/or distributed defense strategies based on the theoretic work.