The effectiveness of game theory in network security is being researched extensively by modeling the attackers and defenders as players interacting in a game.

We propose a preliminary study towards building a game inspired defense architecture (GIDA) which aims to provide quantifiable defense mechanisms to real world security problems by modeling them as multi-player games.

We demonstrate the applicability of our defense architecture using a distributed denial of service attack scenario and verify its effectiveness via simulation.

**Game Inspired Defense Architecture**

Our architecture consists of a Game Decision System and a Game Repository.

The Game Decision System (GDS) is used to compare potential game models for a particular attack and execute the one which is most relevant. GDS consists of:

1. A taxonomy of game related metrics called Attack-Defense and Performance metric Taxonomy (ADAPT) [1]
2. A Game Assessment Algorithm for comparing potential game models to pick the one which is most beneficial to the defender.

**Game Assessment Algorithm**

The Game Assessment Algorithm takes game models as its input and uses ADAPT to provide a relevance score R for each game model. This score is based on the relevance between attack components and game model components.

Attack components represent the different kinds of impact an attack can have on a target system. Game model components correspond to the attack components of the attack they address.

Game model with the highest score is selected and then used by GDS for defense. We explain this algorithm below using a DDoS attack scenario.

### Input:
- A set of game models J, J = a set of attack components c_j

### Output:
- A game model j best suited for defense

**Game Assessment Algorithm**

1. for each ith attack component c_j
2. identify its corresponding metrics c_j(a_j,p)
3. end for
4. Initialize the relevance score R = 0 for all game models j ∈ J
5. for each game model j ∈ J
6. for each game model component c_j in j
7. compute component relevance score R_j based on c_j(a_j,p)
8. end for
9. end for
10. Add the component relevance score for each game model to R_j
11. Return game model j with the highest relevance score R_j

**Attack Scenario: Distributed Denial of Service (DDoS)**

**Drop Flow**

At the Gateway

- PR -> P1

If each node costs $x to acquire and use, then the attacker has to spend m * x in total, where m is # of attack nodes.

\[(att\_cost) = m \times x\]

The metric “resources used by the attacker (att\_res) = quantitatively reflects the number of nodes used by the attacker, which is m.

\[(att\_res) = m\]

Since the rate of occurrence of the attack is directly proportional to the number of nodes being employed by the attacker, the metric “average rate of occurrence (AR0)" correlates to the component \(v_c\).

\[(AR0) = \frac{m}{r}\]

Where \(r\) is a constant. Since game model 1 accounts for these metrics by its third component and game model 2 does not, the game model 1 addresses the attack more comprehensively when compared to game model 2.

That is, game model 1 is more relevant to the attack than game model 2 by the value of \((att\_cost, att\_res, AR0)\)

\[R_1 - R_2 = (att\_cost, att\_res, AR0)\]

Thus by using the game model 1, the defender would be able to defend the attack better than when compared to game model 2.