The Network Security Problem from a Game Theoretic Approach

Laura Gutierrez Funderburk

September 26, 2017

Abstract

Network security is a complex and challenging problem. Researchers have been exploring the applicability of game theoretic approaches to address the network security issues [1]. In this essay, we explore existing approaches to model the Network Security problem using Game Theory. We also mention some of their current limitations. Furthermore, we model this problem as a static game with complete and imperfect information where the players are an attacker, a network administrator and user. In this model, we assume an attack has taken place and create different scenarios where user and network administrator interact on two different levels: policy implementation and communication. We conclude networks are more likely to deflect an attack if the users and administrator play cooperative games.

1 Introduction [1],[6]

As networks play an increasingly important role in modern society, we witness the emergence of new types of security and privacy problems that involve direct participation of network agents. Such agents are individuals, as well as devices or software, selfish or malicious. Consequently, there is a fundamental relationship between the decision making of agents and network security problems.

The weakness of the traditional network system solutions is that they lack a quantitative decisions framework. As Game Theory deals with problems where multiple players with contradictory objectives compete with each other, it can provide us with a mathematical framework for analysis and modelling network security problems. As an example, a network administrator and an attacker can be viewed as two players participating in a non-cooperative game. Whereas there is extensive research on models that explore this setting, to my knowledge there are not nearly as many exploring games which include network users as part of the game. What I propose in this essay is the modelling the network security problem as a game that involves cooperative and non-cooperative actions between network users, network administrator and an outside attacker.

2 An overview of Game Theory [6]

Game Theory describes multi-person decision scenarios as games where each player chooses actions which result in the best possible rewards for self, while anticipating the rational actions from other players.

A player is the basic entity of a game whi makes decisions and then performs actions. A game is a precise description of the strategic interactions that includes the contstraints of, and payoffs for, actions that the players can take, but says nothing about what actions they actually take. A *solution concept* is a systematic description of how the game will be played by employing the best possible strategies and what the outcomes might be.

A Nash equilibrium is a solution concepts that describes a steady state condition of the gamel no player would prefer to change his strategy as that would lower his payoffs given that all other players are adhering to the prescribed strategy.

3 Definitions [6]

Game
A description of the strategic interaction between opposing, or co-operating, interests where the constraints and payoff for actions are taken into consideration.

Player
A basic entity in a game that is tasked with making choices for actions. A player can represent a person, machine, or group of persons within a game.

Action
A move in the given name.

Payoff
The positive or negative rewards to a player for a given action within the game.

Strategy
Plan of action within the game that a given player can take during game play.

Perfect Information Game
A game in which each player is aware of the moves of all other players that have already taken place. A game where at least one of the players is not aware of the moves of at least one other player that have taken place is called an Imperfect Information Game.

Complete Information Game
This is a game in which every player knows both the strategy and payoffs of all players in the game, but not necessarily the actions. This is different from from Perfect Information games in the fact that it does not take into account the actions each player has already taken. Incomplete information games are those in which at least one player is unaware of the possible strategies and payoffs for

at least one of the other players.

Bayesian Game
A game in which information about the strategies and payoff for other players in incomplete and a player asigns a 'type' to other players at the onset of the game.

Static/Strategic Game
A one-shot game in which each player chooses his plan of action and all player's decisions are made simultaneously.

Dynamic/Extensive Game
A game with more than one stage in each of which the players can consider their action. It can be considered as a sequential structure of the decision making problems encountered by the players in a static game. The sequences of the game can either be finite, or infinite.

Stochastic Game
A game that invoved *probabilistic transitions* through several states of the system. The game progresses as a sequence of states. The game begins with a start state; the players choose actions and receives a payoff that depend of the current state of the game, and then the game transitions into a new state with a probability based upon player's actions and the current state.

4 A summary of existing approaches and models [6]

In this section, we explore some of the existing models that fall under the category of non-cooperative games. Furthermore, we provide a few examples of existing models with a focus on static games with complete, incomplete and imperfect information.

4.1 Taxonomy: Classification of current research

Game Theory:

1. Non-Cooperative Games
1.1 Static Games
1.1.1 Complete and Imperfect Information
1.1.2 Incomplete and Imperfect Information
1.1.2.1 Bayesian Formulation
1.1.2.2 Non-Bayesian Formulation
1.2 Dynamic Games
2. Cooperative Games

The existing game-theorecit research as applied to network security falls under non-cooperative games.

4.2 Static Games

All static games are of imperfect information. According to the completeness of information, static games can be classified in two sub-classes as listed below.

4.2.1 Complete imperfect information

Jormokka et al.[3] introduced a few examples of static games with complete information where each example represents an information warfare scenario. The authors investigated if more than one Nash equilibria exist and if so, then which one is most likely to appear as the outcome given the player's strategies.

Carin et al. [9] presented a computational approach to quantitative risk assessment for investment efficient strategies in cyber security. The focus of their work was how to protect the critical intellectual property in private and public sectors assuming the possibility of reverse engineering attacks. They proposed an *attack/protect economic model* cast in a game theoretic context.

4.2.2 Incomplete imperfect information

Liu et al [4] presented a methology to model the interactions between a DDoS attacker and the network administrator. This approach observed that the ability to model and infer attacker intent, objectives and strategies (AIOS) is important as it can lead to effective risk assessment and harm prediction. The work also observed that the best game model to choose depends on the degree of accuracy of the employed IDS and the degree of correlation among the attack steps.

Liu et al [5] focused on the intrusion detection problem in mobile and ad-hoc networks. Their two-player game model is based on a Bayesian formulation and they analyzed the existence of Nash equilibria in static scenario. This work investigated the Bayesian Nash Equilibria (BNE) in the static model. The authors also presented some results from the experiments performed on the ns-2 simulator.

4.3 Dynamic Games

A dynamic game can be either of complete or complete information, and may involve perfect or imperfect information. For ach sub-class of dynamic games, we briefly disucss the exisitng research works which fall under the corresponding sub-class.

4.3.1 Complete perfect information

Lye et al [7]. proposed a game model for the security of a computer network. In this work, an enterprise network was envisiond as a graph of 4 nodes (web server, file server, work station and external world) along with the traffic state for all the links. It is a two-player (administrator, attacker), stochastic, general-sum game and the authors focused on three attack scenarios, namely, defaced website, denial-of-service, and stealing confidential data. The game was described from the point of view of both players. A formal model defined the game as a 7-tuple - the set of network states, the action set for each player, the state transition

function, the reward function and a discount factor This work considered a stochastic game involving 18 netowrk states and 3 actions for each player at each state. With different initial conditions a set of Nash Equilibria were calculated using Matlab.

4.3.2 Complete Imperfect Information

Alpcan et al [8] modeled the interaction between malicious attackers to a system and the IDS using a stochastic (Markov) game.They consider three different information structures:

(a) The players have full information about the sensor system characteristics and the opponents,

(b) the attacker has no information about the sensor system characteristics,

(c) each player has only information about his own costs, past actions and past states.

4.4 Limitations of these models

Many of the current game-theoretic security approaches are based on either static game models, or games with perfect information, or games with complete information. However, in reality a network administrator often faces a dynamic game with incomplete and imperfect information against the attacker. Some of the current models involving dynamic game with incomplete and imperfect information are specific to wireless networks while a few others do not consider a realistic attack scenario.

Some of the limitaions of the present research are:

(a) Current stochastic hame models only consider perfect information and assume that the defender is always able to detect attacks;

(b) Current stochastic game models assume that the state transition probabilities are fixed before the game starts and these probabilities can be computed from the domain knowledge and past statistics;

(c) Current game models assume that the player's actions are synchronous, which is not always realistic;

(d) Most models are not scalable with the size and complexity of the system under consideration.

Furthermore, these models presupose only a network administrator and an attacker play. But in reality, network users play an important role in how successful a given attack can be.

In the next session, we model a game and claim that users that cooperate with the network administrator, operate in a stronger, more secure network, than users who play non-cooperative games with the network administrator.

5 The network security problem modelled as a game between user and network administrator against attacker

5.1 Definitions

Policy is the set of rules in place for users to participate in the network. A good policy is one that allows users to perform their work without compromising security. A bad policy is one that either does not let users to perform their work, or is not strong enough to protect the network from known attacks.

5.2 Assumptions

We assume this game to be static of complete and perfect information.

We also assume in this game that network policy is 'good enough' to protect from common attacks, and that a bad policy is one which is not user-friendly.

5.3 Proposed model

We model the network security problem with three players as an interdependent game as follows:

Player 1. Network administrator. Goal is to protect network and provide service to users.

Player 2. Outside attacker. Goal is to damage the network.

Player 3. Network user. Goal is to use network to perform their work. Note that in this model we use the word 'user' to refer to all members of the network.

We model the interactions of network administrator and attacker as a non-cooperative game, and we claim that the failure of a network administrator in defending the network against attacks, is influenced heavily on playing a non-cooperative game with network users.

We define some of user's and administrator's actions as follows:

Network administrator plays two roles:

(a) Maintain network. Administrator is given -1 points any time he/she is able to succeed and $+1$ otherwise.

(b) Provide service to user. Administrator is given -1 whenever the user's needs are satisfied in time, and $+1$ otherwise.

Network user plays two roles as well:

(a) Uses the network to perform work under network policy. Anytime the user

respects the policy implemented by the administrator he/she is given -1 point, and $+1$ otherwise.

(b) Communicates with network administrator for anything related to the use of their workstation. Whenever a user reports a problem to the administrator in a clear way, they are given -1 and $+1$ otherwise.

5.4 Policy implementation and usage as a game

We can then model this problem as follows. Each cell contains the number of points that each players gains or looses multiplied by a variable $t > 1$ denoting the time is lost or gained in the event of an attack. We first model the policy game between administrator and user. In this game the user's success and failure (denoted as S and F respectively) depends on its ability to follow the policy. The success of the administrator depends on its ability to craft and implement a policy that is effective in protecting the network as well as allowing the user to perform their work.

Note that in this model, a negative time indicates a gain and a positive time indicates a loss.

		Admin (y player)	Admin (y player)
		S	F
User (x player)	S	(-t,-2t)	(-t,2t)
User (x player)	F	(t,-2t)	(t,2t)

Let's break down how this works. In the event that the policy is successful **and** the user follows it, users gain time in performing their work, and network administrator gains time in defending himself against an attack.

In the event that the administrator fails to implement a good policy but the users follows it anyway, in the event of an attack, the network is less likely to fall from a blow given that a user who cooperates is less likely to introduce additional vulnerabilities. The downside in this scenario is that, overtime users begin to perceive network administrator as slow and not helpful. Overtime this scenario will cause friction and eventually lead to the user not wanting to cooperate.

If the policy is good, but the user decided not to follow it, then the user may have a gain of time at first, but when the network administrator finds out they will have to waste time being penalized for their action.

In the last scenario both the users and the administrator failed in their respective roles, and as a byproduct the network is now an easy target for attacks. On the one hand, users acting with no consideration for others are more likely to introduce additional vulnerabilities into the network, and on the other a network administrator who is unable to implement a good policy will create an environment where users perceive him/her as a threat to their progress.

5.5 Network admin and user communication as a game

We now model the communication game as follows: suppose an attack has taken place. And the network administrator needs to know with as much detail as possible, where the infected node is, who the last user was, what action was performed, what programs where involved, and any additional information that might be useful. To make the game more interesting, suppose the network administrator needs to exchange details with the user, that is, suppose there is no automated system providing all infromation.

In this game, the network admin is given -1 points if he/she succeeds in detecting network attack, and $+1$ otherwise.

Similarly, user is given -1 if they cooperate, that is if they communicate all they know with clarity and honesty, and $+1$ otherwise.

Just like in the previous model, we multiply by a variable $t > 1$ where t denotes time. A negative time indicates a gain, while a positive time indicates a loss.

		Admin (y player)	Admin (y player)
		S	F
User (x player)	S	(-t,-t)	(-t,t)
User (x player)	F	(t,-t)	(t,t)

As we can see, in the event of an attack, when user and administrator collaborate both gain time as the network administrator can more quickly implement an adequate solution and the user can go back to their duties.

If the administrator fails to detect an attack immediately, but the user collaborates and provides as much detail as necessary of all they know, then there exists a higher probability an adequate solition can be found.

Similarly, if the network admin detects an attack but the user refuses to cooperate, then the admin must spend time troubleshooting in hope of finding the cause of the problem.

The last scenario is by far the worst, for it presuposes that neither the admin detects an attack nor the user communicates what they know. Under these circumstances, the network is taken down by the attacker.

5.6 Remarks

Based on these models we conclude that in the event of an attack, a network administrator is more likely to detect and respond appropriately if user cooperates by communicating and by following policy.

Furthermore we observe that it is crucial for the network administrator to ensure their users are getting the support they need, to avoid giving users the option of not cooperating. We see that if the network administrator is successful in creating a good policy, and keeps open communication with the user, then the likelyhood of a successful attack is lower.

We finalize this section noting that a network where all parties (user and administrator) work towards the same goal and cooperate with one another is much stronger and more likely to defend itself from attacks than a network where users do not cooperate, act in selfish ways as to gain control and in general do not keep in mind that their actions have an impact on everyone connected to the network.

6 Further areas of work

This model is limited in that it assumes interactions are static, with perfect and incomplete information. Furthermore, it assumes all users within a setting act as one. In reality each user provides a unique set of opportunities and challenges, where each user comes with different levels of technical knowledge, communication skills, deadlines and priorities. In addition to this, this model does not take into account differences in personality, likes and dislikes, in addition to disagreements, which also form a crucial part of some of the non-cooperative games that user and network administrator can sometimes play with one another.

7 Bibliography

[1] Manshaei, M. H., Zhu, Q., Alpcan, T., Başar, T., and Hubaux, J.-P. 2013. Game theory meets network security and privacy. ACM Comput. Surv. 45, 3, Article 25 (June 2013), 39 pages. DOI: http://dx.doi.org/10.1145/2480741.2480742
[2] Interdependent Relationships in Game Theory: A Generalized Model. Li, Jiawei. January 2016. arXiv:1601.00176
[3] J. Jormakka and J. V. E. Molsa. Modelling information war- fare as a game. Journal of Information Warfare; Vol. 4(2), 2005.
[4] P. Liu, W. Zang, and M. Yu. Incentive-based modeling and inference of attacker intent, objectives, and strategies. ACM Transactions on Information and System Security (TISSEC), 2005. [5] Y. Liu, C. Comaniciu, and H. Man. A bayesian game ap- proach for intrusion detection in wireless ad hoc networks. ACM International Conference Proceeding Series; Vol. 199, 2006.
[6] A Survey of Game Theory as Applied to Network Security Sankardas Roy, Charles Ellis, Sajjan Shiva, Dipankar Dasgupta, Vivek Shandilya, Qishi Wu
[7] K. Lye and J. Wing. Game strategies in network security.
[8] T. Alpcan and T. Baser. An intrusion detection game with limited observations. Proc. of the 12th Int. Symp. on Dy- namic Games and Applications, 2006.
[9] L. Carin, G. Cybenko, and J. Hughes. Quantitative evalua- tion of risk for investment efficient strategies in cybersecu- rity: The queries methodology. IEEE Computer, 2008.