2019-2020
ANKARA UNIVERSITY
DEPARTMENT OF COMPUTER ENGINEERING
COM445 INFORMATION SYSTEMS

A Dynamic Game Approach to Strategic Design of Secure and Resilient Infrastructure Network Paper Analysis Report

16290125 Karanfil Eylül ŞENGÜN, 16290085 Yeter Tuğba ÇETİN,
15290134 Sercan Yılmaz

1. INTRODUCTION

An organization's agility and efficiency are not based solely on hard-working workers and excellent equipment. Smooth operation requires a robust, clean, secure and available network infrastructure. Network infrastructure refers to a network that enables network or internet connectivity, management, business operations, and communication. A network infrastructure usually consists of both hardware and software.

The vulnerabilities of infrastructure network systems are the focus of several initiatives around the world. This is the result of the awareness about the urgency of the matter and that is why these problems must be handled. Infrastructure networks have not only physical but also cybersecurity vulnerabilities. Most security vulnerabilities in infrastructure include failures to adequately define security sensitivity for automation system data, identify and protect a security perimeter, build comprehensive security through defense-in-depth, and restrict access to data and services to authenticated users based on operational requirements [1]. The paper that we are going to brief adopts a strategy that is being used in dynamic game theory. The usage of this theory aims to prevent inaccessibility between data and network components. The paper claims that one way to protect the network is by creating redundant links in the network. In this way, if the links are arbitrarily removed, the connection continues uninterrupted. This is an effective approach, but it can have very high costs. Therefore, while having limited budget and resources, optimal attack and post-attack security mechanisms should be developed.

In the article, a two-player dynamic three-stage network game formation is established. The first player is the designer, denoted by D, who aims to create a network between different nodes and protect this network against a malicious attack. Also after an attack, it will try to heal the network by creating new links and keep the connectivity established before and after the attack. An adversary, denoted by A, puts an attack on the network by removing a subset of its links. The designer should also consider that the attacker may attack again even before the healing stage starts. We should keep in mind that each player has a cost on creating or removing links. Therefore, strategic decisions are crucial for maintaining and recovering infrastructure at minimum cost. In the first phase of the game, the designer creates a network

of unnecessary links to deter adversarial behavior. In the second stage, the attacker achieves maximum disconnectivity by destroying the minimum number of links to minimize the cost. In the final stage of the game, the designer can repair the network by adding new links. In the paper as the solution concept, the subgame perfect Nash equilibrium (SPE) is adopted.

The Nash equilibrium is a concept of game theory where the optimal outcome of a game is one where no player has an incentive to deviate from his chosen strategy after considering an opponent's choice. A Nash equilibrium is said to be subgame perfect if an only if it is a Nash equilibrium in every subgame of the game. We can use this short-story analogy to understand the concept better: *"If we all go for the blonde and block each other, not a single one of us is going to get her. So then we go for her friends, but they will all give us the cold shoulder because no one likes to be the second choice. But what if none of us goes for the blonde? We won't get in each other's way and we won't insult the other girls. It's the only way to win. It's the only way we all get laid."* [2]

2. THE BRIEF EXPLANATION OF DYNAMIC GAME FORMULATION

The Infrastructure system is considered to be a system represented by *n* nodes. In the previous section, we talked about the roles and actions of the players. In addition, the appropriate time for the actions to take place plays a very important role. There are some abbreviations that are used to describe the parameters of the game theory.

- $\mathcal{E}_1$: the set of links created by the defender at time 0.
- $\mathcal{E}_A$: the set of links attacked by the adversary.
- $\mathcal{E}_2$: the set of links created by the defender after the attack.
- C_D (respectively C_A): unitary cost of creating (respectively removing) links.
- 1_E means that at any set $\mathcal{E}$ if the network graph is connected, it is equal to 1 and 0 otherwise.
- τ: attack time of the adversary.
- τ_R: the time passed, after the attack and the network recovery by the defender.
- U_D (respectively U_A): the utility of defender (respectively adversary).

Since both players are strategic, SPE analyzes the strategies of the players. It involves three sequentially nested problems, starting from the third stage to the first stage. The first protection problem is: The defender wants to achieve the highest utility it can obtain. During the healing, it tries to work the minimum cost. The second problem is: Just like the defender, the adversary wants to obtain the highest utility too by selecting the minimum number of links to be eliminated and unlike the defender, the attacker aims not to lose the gain from the links it has eliminated until the healing process during the healing process initiated by the defender. And the last problem is: The defender must create a network so that the adversary's possible attack points should be minimized. SPE solves all these problems that are mentioned above.

In epitome, it is assumed that the defender knows the attack time and attack cost. However, in practice designer may have no information about the parameters of the attacker. The designer can attempt to calculate these values for the attack's estimation. But the adversary's behavior may not be the same as expected. Thus, the defender needs a recovery strategy at

time τ. Since this also leads to an optimization problem, a dynamic bayesian game makes the solution important by randomizing the parameters.

3. POSSIBLE CONFIGURATIONS OF SPE

There are seven lemmas to analyze the configuration of infrastructure networks. During the analysis, C_D should not be too large so that D can create a network. In order for an attacker to be a competitor to the defender, the cost of the attack must not be too high:

Lemma 1. At τ^{th} time, if the C_A is too high A has no intention to attack. If A attacks, since its utility will be negative, this will not be a logical action. Similarly, if C_D is too high, the defender will bound the network with the minimum number of links.

Lemma 2. ε_1, ε_A, and ε_2 can have up to 8 states.

Situation	Connected	Ratio of Attack	Ratio of Healing
1	1	1	1
2	1	0	1
3	1	0	0
4	0	0	1
5	0	0	0

As shown in the table, there are no attacks in cases 4 and 5 because there is no connected network. The structure of the SPE depends on the data in the table above. As a result, the healing depends on the adversary's intent. We can list this situation under two main headings;

1. The defender can make healing after $\tau + \tau_R$ time:

   In this situation, the paper suggests that while using the *Harary network*, if the attacker destroys the k link, we only need to create a $\left\lceil \frac{(k+1)n}{2} \right\rceil$ network with links to keep the connectivity where n is the number of nodes being resistant to k attacks. It also supports this idea using *tree networks*. The direct consequences of the situations are as follows,

   a) If the attacking cost is too much, U_D is only the cost of the initial cost of links.
   b) If the recovery is successful after the adversary attacks, the attacker will not be able to make any gains. Defender, on the other hand, has to cover the initial cost of initial link creation and recovery after the attack.
   c) If the C_D is high, the defender will not be able to compensate for any lost link. This gives the attacker a utility as much as $\tau_R - C_A$. The defender has to cover the costs of the lost links in addition to the previous situation.
   d) Lastly, if the defender has too high costs to heal, the attacker will gain all the links it has destroyed. Defender, on the other hand, has to pay initial creation and loss costs since it does not make any healing.

   Lemma 3. states the correctness of these consequences using various examples.

2. The defender does not heal all of the links after $\tau + \tau_R$ time:

   D reconnects k links where k is equivalent to $\left\lfloor \frac{1-\tau-\tau_R}{c_D} \right\rfloor$

   Lemma 4. According to the second deduction, there are three results that are obtained to define the potential best response strategies of A to the links that are created in the first phase:

   a) A decides not to attack so that U_A will be 0.
   b) A attacks many links but only disconnects the minimal number of links. D heals the network by constructing only one link, then A only gets paid for these links.
   c) If A attacks k+1 links then D will not heal the network. Thus, A receives the utility of all the destroyed links.

   Lemma 5. states that the best time for the defender to start the healing is $\tau + \tau_R$ under the conditions that are discussed in it. This provides D the best time to heal the network with a minimum number of links.

   Lemma 6. says that defender plays a leading role in the strategies that the opponents will determine in order to obtain the highest utility. Accordingly, the attacker will choose the SPE that will bring its payoff to the highest level. However, A may have some constraints while attacking. Some links may not be compromised by A. These links are called *secure links.* Not every link needs to be a secure link because connectivity can also be provided by creating supernodes. Figure 6 from the article illustrates this situation with an example.

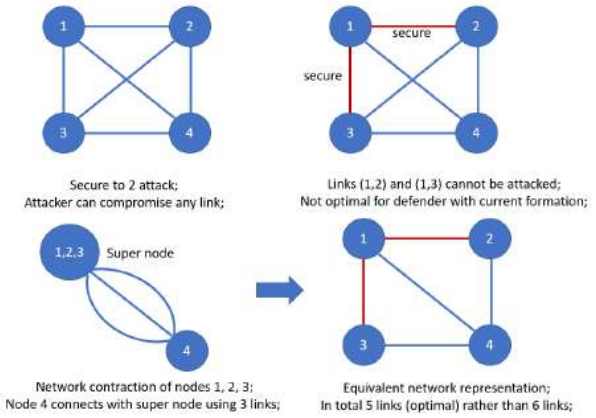

Fig. 6: Illustration of network contraction for designing D's optimal strategy when a subset of nodes can form secure links with others. In the example, 6 links are required for the network being resistant to 2 link removals if A can compromise any link. When links (1,2) and (1,3) cannot be attacked, nodes 1, 2, and 3 can be aggregrated as a super node by network contraction. Then, node 4 connects with the super node using 3 links. In sum, 5 links are sufficient for this constrained scenario which is different from the unconstrained case.

   Lemma 7. In addition to the aforementioned lemmas, the time it takes for the response and recovery after an attack and the strategic timing of this attack is also a critical issue and it differs according to the situations. These values can be determined by analyzing the potential optimal utilities and τ varies to account for the better recovery speed τ_R and the increasing cost of attack.

To corroborate the obtained analytical results discussed above, the paper uses a case study about disaster recovery in UAV-enabled communication networks for a better illustration. In a nutshell, the dynamic game approach provides the defender a better payoff with a higher level of resilience by saving link resources and creating a securely connected infrastructure yet, a longer duration between the attack and recovery phases increases the cyber threats to the infrastructures.

On the other hand, the paper is insufficient to explain the situations where there are scenarios that the attacking time and cost are known but the defender's information is incomplete. Also, SPE strategies where both defender and attacker are constrained are not discussed.

4. CONCLUSION

In game theory, players are only aware of the strategies that are against their known strategies. In real life, there could be strategies that we can not estimate at all. We can easily understand the game that has been mentioned in the paper, however, the theory of the games has not been developed with more than four players. For instance, if the number of attackers increases, the defender will be insufficient to estimate all of the strategies. Also, game theory suggests that opponents will always make a wise move and adopt a countermove. According to the famous game theorist Ariel Rubenstein, *"On theory, payoffs are only represented by the monetary amount that the player receives. In practice, as is seen from the Ultimatum Game, payoffs also include emotions such as spite. … Logic is a very interesting field in philosophy, or in mathematics. But I don't think anybody has the illusion that logic helps people to be better performers in life. A good judge does not need to know logic. It may turn out to be useful – logic was useful in the development of the computer sciences, for example – but it's not directly practical in the sense of helping you figure out how best to behave tomorrow, say in a debate with friends, or when analyzing data that you get as a judge or a citizen or as a scientist."* [4]

From our perspective, in parallel with his thinking, we think that logic is sometimes useful in determining a specific strategy to use, but it is not always so useful in discussions with friends or analyzing information based on real-life events. Although the facts are revealed before you, it is impossible to perfectly predict human emotions and other intangible factors. These unpredictable factors are inadequate in game theory applications. Basically, people are not always rational. Although Rubenstein has made a rightful point, despite these limitations, game theory helps provide solutions to some of the complex problems even though as a mathematical technique, it is still in its development stage. That is why for future movements and their costs that can occur game theory has effective solutions to ensure maximum benefit in many different domains such as economy, market shares, war strategies, relationships among persons and the subject of the paper, cybersecurity in infrastructures. One such proposition, which is currently being explored by researchers, is the use of linear programming. The integer programming can be used to provide a practical solution to DDoS attacks.

Linear programming is a simple technique where we depict complex relationships through linear functions and then find the optimum points. The important word in the previous sentence is 'depict'. The real relationships might be much more complex – but we can simplify them to linear relationships. [5] Using linear programming methods for infrastructure network security issues caused by traffic congestion, we can optimize the game theory into real life in a more efficient way.

REFERENCES

Related Paper: A Dynamic Game Approach to Strategic Design of Secure and Resilient Infrastructure Network, Juntao Chen, Corinne Touati, Quanyan Zhu, IEEE Transactions on Information Forensics and Security, June 2019, https://arxiv.org/abs/1906.07185

[1] Common vulnerabilities in critical infrastructure control systems. Jason Stamp, John Dillinger, William Young, and Jennifer DePoy. SANDIA Corporation, 2003.

[2] https://medium.com/cantors-paradise/the-nash-equilibrium-explained-c9ad7e97633a

[3] https://blog.gigamon.com/2019/03/06/what-is-network-infrastructure/

[4] https://mostlyeconomics.wordpress.com/2012/06/08/why-study-game-theory-when-it-has-limited-practical-applications-in-real-life/

[5] https://www.analyticsvidhya.com/blog/2017/02/lintroductory-guide-on-linear-programming-explained-in-simple-english/