Journal of Information Security, 2010, 1, 41-44
doi:10.4236/jis.2010.11005 Published Online July 2010 (http://www.SciRP.org/journal/jis)

Game Theory Based Network Security

Yi Luo[1], Ferenc Szidarovszky[1], Youssif Al-Nashif[2], Salim Hariri[2]
[1]*Department of Systems and Industrial Engineering, University of Arizona, Tucson, USA*
[2]*Department of Electrical and Computer Engineering, University of Arizona, Tucson, USA*
E-mail: *Luo*1*@email.arizona.edu*, *szidar@sie.arizona.edu*, {*alnashif*, *hariri*}*@ece.arizona.edu*
Received March 9, 2010; *revised July* 9, 2010; *accepted July* 20, 2010

Abstract

The interactions between attackers and network administrator are modeled as a non-cooperative non-zero-sum dynamic game with incomplete information, which considers the uncertainty and the special properties of multi-stage attacks. The model is a *Fictitious Play* approach along a special game tree when the attacker is the leader and the administrator is the follower. Multi-objective optimization methodology is used to predict the attacker's best actions at each decision node. The administrator also keeps tracking the attacker's actions and updates his knowledge on the attacker's behavior and objectives after each detected attack, and uses it to update the prediction of the attacker's future actions. Instead of searching the entire game tree, appropriate time horizons are dynamically determined to reduce the size of the game tree, leading to a new, fast, adaptive learning algorithm. Numerical experiments show that our algorithm has a significant reduction in the damage of the network and it is also more efficient than other existing algorithms.

Keywords: Multi-Stage Attack, Dynamic Game, Multi-Objective Optimization, Adaptive Learning

1. Introduction

The increased dependence on networked applications and services makes network security an important research problem. Detection of intrusions and the protection of the networks against attacks is the central issue. Game theory is an appropriate methodology to model the interactions between attackers and network administrator and to determine the best countermeasure strategy against attacks. There are however some difficulties in directly applying classical game theory, since the attackers' strategies are uncertain, their steps are not instantaneous, the rules of the games might change in time, and so on. Therefore any game theory based methodology has to take these difficulties into account.

There are many types of intrusions. Multi-stage attacks are the most destructive and most difficult kinds for any defense system. They use intelligence to strategically compromise the targets in a planned sequence of actions, so the usual methodology designed to protect against single-stage attacks cannot be used.

Network intrusion response mechanisms have been intensively developed and studied in recent years. Several authors used Markov Games (MG) as a model and methodology. Lye and Wing [1] viewed the interactions between the attacker and the administrator as a two-player Markov game and modeled it by an intrusion graph. The recovery effort was considered as the cost of the response. The payoff for the attacker was defined by the amount of effort the administrator needed to spend in order to bring the network back to normal state. The equilibrium was obtained by using nonlinear programming and dynamic programming for infinite and finite horizon games, respectively. The main disadvantage of this approach is the huge size of the state space which makes extremely difficult to compute the equilibria. Shen *et al.* [2] used a piecewise linearized Markov game model with estimated beliefs of the possible cyber attack patterns obtained by data fusion and adaptive control. They also recognized that larger time-step horizons result in increased computation complexity. Another approach is based on Partially Observable Markov Decision Processes (POMDP) which results in more complex computation problems. Carin *et al.* [3] introduced the protection map and used reverse-engineering methodology to build an attack graph. Zhang and Ho [4] presented a model to characterize multi-stage collusive attacks in terms of key spatio-temporal properties. The attacker's behavior was modeled as a reward-directed partially observable Markov

The research presented in this paper is supported in part by National Science Foundation via grants numbers CNS-0615323 and IIP-0758579, and by Electronic Warfare Associates, Inc. via the grant number ewagsi-07-LS-0002, and it is conducted as part of the NSF Center for Autonomic Computing at University of Arizona.

decision process and the administrator was assisted by identifying the potential causal relationships between the different system vulnerabilities. This approach also suffered from serious computation difficulties because of the very large state space. Liu *et al.* [5] introduced a dynamic game approach based on modeling the Attacker Intent, Objectives and Strategies (AIOS) which resulted in a much smaller state space, so this approach is more efficient than the application of Markovian games. A similar concept was applied in Siever *et al.* [6] for the security of electric power transmission grids, when the goals of the attacker were used in formulating the attacker's game, which optimizes the difference of its reward and the amount of power delivered. The objective function of the defender is the sum of the amount of delivered power and a special reward function. The approach introduced by Luo *et al.* [7] was based on POMDP, however a reduced special game tree structure was used and a new stochastic multi-stage defense algorithm was developed.

All models and algorithms are based on assessing all damages and costs of the cyber attacks. The uncertainty in the knowledge of the network, its vulnerabilities, possible actions and counteractions, damages and costs, etc. make the mathematical modeling more complicated. In the economic literature this issue has been known and treated by the deterministic equivalent, which is a linear combination of the expected value (μ) and variance (σ^2) of a random outcome: $\mu - \alpha\sigma^2$, where α shows the level of willingness of the decision maker to take risk.

Almost all models of multi-stage attacks are based on special game trees. It is well-known from the game theory literature (see for example, Forgo *et al.*, [8]) that such games with full information always have at least one Nash equilibrium, which can be computed by using backward induction. This general result however cannot be used in computer network security, since the game tree and the possible strategies of the players are not completely known by all participants. The administrator and the attacker might believe in different game trees with different possible actions.

2. Consequence Modeling

We have adopted the approach given in Richardson and Chavez [9]. The consequence of any attack and any action during a multi-stage attack is based on the following six steps:

1) Define the categories of impact;

2) State the importance of each category relative to the others;

3) Define the measures of impact for each category;

4) Define the relationships between physical effects and impact measures;

5) Define the system and its users;

6) Define the events in terms of scales and network system impact.

Impact categories include and not restricted to economic, image, safety, security, intelligence, and privacy concerns. Their relative importance factors can be assessed by any one of the well known procedures from multi-criteria decision making (see for example, Szidarovszky *et al.*, [10]). A common approach of obtaining the weights is based on pair-wise comparisons, when all participants in the decision making process are asked to give relative importance factors for all pairs of categories. Then the results are summarized into a final set of importance weights either by averaging them or by using the Analytic Hierarchy Process (AHP). The measures of the impact in different categories are usually given in different units, and they can be combined by using multi-attribute utility theory or weighting method with normalized evaluations. Performance measures can be defined for the impact categories, and each performance measure can be divided into a set of constructed scales representing the amount of impact the physical consequences have on the network and its users including lost revenue, repair and/or replacement cost, damage by lost or stolen information, etc. Any actual attack has impacts on different categories with different levels. Using the consequence modeling tool, the overall consequence of the different types and scales of events on the system and its users can be assessed into one combined value. This value has to be computed at all states of the multistage attack and will be used in the game tree analysis.

3. Game Tree and Decision Nodes

Multi-stage attacks are represented by special game trees. **Figure 1** shows the first two interactions on a game tree. The attacker is the leader, the administrator is the follower. The root of the tree is the initial decision node of the attacker, and the possible initial moves of the attacker are represented by the arcs originating at the root. These actions might include attacking the server with different intensity levels, sending a virus to a group of customers, etc. At the end point of each arc the administrator has to

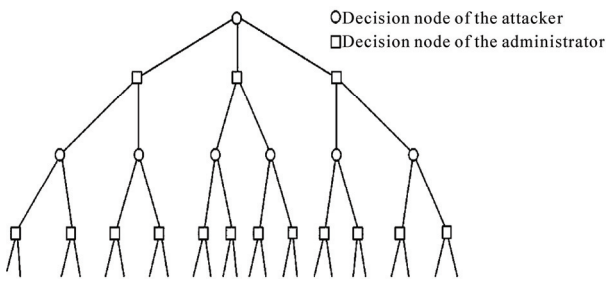

Figure 1. Special game tree.

respond, so they are its decision nodes. After the administrator's response the attacker makes the next move, and so on. This tree continuous until the intruder gives up the attack or reaches its goals. This tree can become very large and the payoff values at the decision nodes are uncertain, therefore the classic method, known as backward induction, cannot be used in this case.

4. Determining Optimal Responses

The algorithm to be described in this section is an on-line procedure, it provides the best response of the administrator at each of its decision nodes, when a multi-stage attack reaches that particular node of the game tree. So during an attack the algorithm can be used at each stage to find the best next move of the administrator starting just after the first action of the attacker and continuing until the end of the game.

Consider now a particular decision node of the administrator and the sub-game tree having this node as its root. The time horizon for this sub-game tree is obtained as follows. We have to check all end points of this sub-game tree where the attacker reaches its goals during smallest number of steps, so we select the shortest path with smallest number of arcs from the root to such end points. The length of the shortest path is the time horizon, and then all paths starting at the root will be considered only until this time horizon. The utility function of the attacker is then assessed at all endpoints of this truncated sub-game tree. The utility function is the linear combination of the expected payoff of the attacker and its variance as it was explained earlier. The risk taking coefficient of the attacker can be updated after each attack, since the administrator has estimates of the expectations and the variances of its utility values for all possible moves and also observes the actual move. The administrator then has to assess the probability distributions of the attacker's actions at all of its decision nodes. The probability values are computed based on the assessed utility values of the intruder as well as previous interactions with the attacker. First the probability values are computed proportionally to the utility values at the endpoints of the different arcs representing the next moves of the attacker, and if previous interactions provide relative frequencies, they are averaged with the computed probabilities. Using these probability distributions the expectation and the variance of the cumulative impact up to the time horizon for the administrator can be computed for each of its possible responses, and the corresponding utility values are obtained by combining expectations and variances with the risk acceptance coefficient of the administrator. The best response of the administrator is the arc which has its highest utility value.

The attacker makes the first move. At the end point of the corresponding arc the administrator has to respond. Using the above procedure the administrator finds its response. Then the attacker makes the next step, and the best next response of the administrator is obtained again by using the same algorithm with updated data based on the information obtained from the previous actions of the attacker. Then the attacker has the next move, the administrator responds by using the same algorithm, and so on until the game ends, which occurs when the attacker stops attacking by reaching its goals or giving up.

5. Numerical Example

Figure 2 shows a network structure. It is assumed that the HTTP server, Database 2, the FTP1 server and the information in the CEO are the vulnerable components in the network system, and access to the information in the CEO is the attacker's objective. It is also assumed that the CEO needs services provided by the HTTP server, Database 2 and the FTP1 server to do its jobs. The attacker can launch multi-stage attacks to obtain the information from the CEO in many different ways. Then the administrator can respond to it by selecting from a set of options, and so on, which leads to the game tree.

Next we assume that in addition to the sensitive data in the CEO the data in the Accounting is another vulnerability of the system. The attacker has now two objectives: the information in CEO and the data in Accounting. The Accounting also needs services provided by Database 2 and the HTTP server, etc. Our computer study assumed that the attacker always selects the action leading to maximal impact, and the administrator always selects its best action at its decision nodes by using one of the three tested algorithms.

We applied three methods to find the best responses of the administrator: One is a greedy algorithm (GA) in which the administrator completely blocks the traffic of

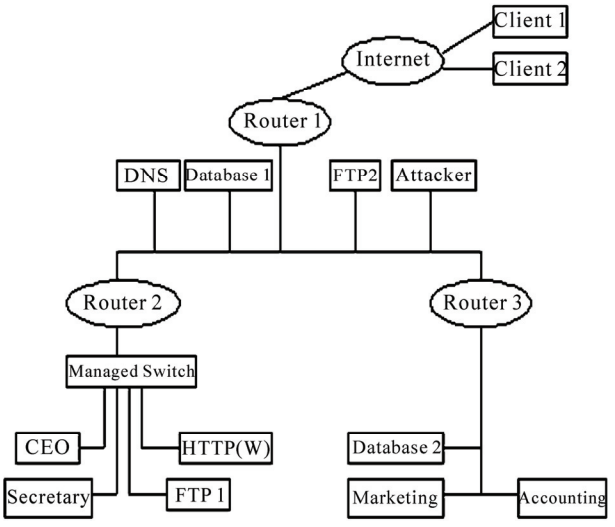

Figure 2. Network structure.

Table 1. The performances of the three algorithms.

The total losses of the system occurred during the life-cycle of the multi-stage attacks			Administrator		
			GA Algorithm	SO Algorithm	Our Algorithm
Attacker	Risk Seeking	Single Objective	4,694	3,608	2,781
		Two Objective	9,597	6,741	4,689
	Risk Neutral	Single Objective	4,694	3,176	2,252
		Two Objective	9,597	6,325	4,021

corresponding services on routers, firewall, or disconnect the machines using managed switches, etc. regardless of what kind of attack occurs or what is the intensity levels of the attack. Another algorithm is also myopic, single-interaction optimization algorithm (SO) in which the administrator tries to minimize the loss from the most current attack at each interaction without considering future interactions with the attacker. The third algorithm is the one we developed. The results are shown **Table 1**. Two types of attacks were assumed. The risk seeking attacker worried about only the expectation of the impact ($\alpha = 0$), while the risk neutral intruder selected a relatively high risk taking coefficient ($\alpha = 1$). The two scenarios refer to the cases of one or two objectives of the attacker. The last three columns indicate the three methods which were used for comparison. The numbers in the last three columns of the table show the total losses of the system with using different methods. Clearly our method resulted in the smallest overall losses in all cases, where the loss reduction was 41%, 51%, 52% and 58% in comparison to the Greedy Algorithm, and 23%, 30%, 29% and 36% in comparison to single-interaction optimization. In assessing the numerical values of the impacts in the consequence analysis, we used only economic impact. A more complex consequence analysis would not alter the main steps of the algorithms.

6. Conclusions

This paper introduced a multi-stage intrusion defense system, where the interactions between the attacker and the administrator are modeled as a two-player non-cooperative non-zero-sum dynamic game with incomplete information. The two players conduct *Fictitious Play* along the game tree, which can help the administrator to find quickly the best strategies to defend against attacks launched by different types of attackers. Our algorithm is an online procedure, which gives the most appropriate response of the administrator at any stage of the game. So it has to be repeated at all actual decision nodes of the administrator. Our algorithm is different than the usual methods based on decision trees, since at each step only a finite horizon is considered, instead of expected outcomes certain equivalents are used and the probabilities of the different arcs are continuously updated based on new information. In our numerical example our approach was compared to two other algorithms and the total network losses were compared. The loss reduction by using our approach varied between 23% and 58%. The performance of our algorithm is much better than that of other algorithms based on the results of our numerical experiments.

7. References

[1] K. Lye and J. Wing, "Game Strategies in Network Security," *International Journal of Information Security*, Vol. 4, No. 1-2, 2005, pp. 71-86.

[2] D. Shen, G. Chen, E. Blasch and G. Tadda, "Adaptive Markov Game Theoretic Data Fusion Approach for Cyber Network Defense," *IEEE Military Communications Conference* (*MILCOM* 2007), Orlando, 2007.

[3] L. Carin, G. Cybenko and J. Hughes, "Cybersecurity Strategies: The QuERIES Methoddology," *Computer*, Vol. 41, No. 8, 2008, pp. 20-26.

[4] Z. Zhang and P. Ho, "Janus: A Dual-Purpose Analytical Model for Understanding, Characterizing and Countermining Multi-Stage Collusive Attacks in Enterprise Networks," *Journal of Network and Computer Applications*, Vol. 32, No. 3, 2009, pp. 710-720.

[5] P. Liu and W. Zang, "Incentive-Based Modeling and Inference of Attack Intent, Objectives, and Strategies," *CCS*'03, Washington, DC., 2003.

[6] W. M. Siever, A. Miller and D. R. Tauritz, "Blueprint for Iteratively Hardening Power Grids Employing Unified Power Flow Controllers," *SoSE*'07, *IEEE International Conference on System of Systems Engineering*, Tampa, 2007.

[7] Y. Luo, F. Szidarovszky, Y. Al-Nashif and S. Hariri, "Game Tree Based Partially Observable Stochastic Game Model for Intrusion Defense Systems (IDS)," *IIE Annual Conference and EXPO* (*IERC* 2009), Miami, 2009.

[8] F. Forgo, J. Szep and F. Szidarovszky, "Introduction to the Theory of Games," Kluwer Academic Publishers, Dordrecht, 1999.

[9] B. T. Richardson and L. Chavez, "National SCADA Test Bed Consequence Modeling Tool," *Sandia National Laboratory Report, SAND*2008-6098, Albuquerque, 2008.

[10] F. Szidarovszky, M. Gershon and L. Duckstein, "Techniques for Multiobjective Decision Making in Systems Management," Elsevier, Amsterdam, 1986.

