
Summary: In the multistep attack scenario, each rational attack-defense player tries to maximize his payoff, but the uncertainty about his adversary prevents him from taking the favorable actions. How to select the best strategy from the candidate strategies to maximize the defense payoff becomes the core issue. For this purpose, the paper innovatively designs a game theory model from the point of network survivability in combination with the attribute attack graph. The attack graph is created based on the network connectivity and known vulnerabilities using the MulVAL toolkit, which gives the full view of all the known vulnerabilities and their interdependence. Then, we use the attack graph to extract attack-defense actions, candidate attack-defense strategies, attack-defense payoffs, and network states, as well as other game modeling elements. Afterwards, the payoffs of attack-defense strategies are quantified by integrating attack-defense strength and network survivability. In addition, we input the above elements into the game model. Through repeated learning, deduction, and improvement, we can optimize the layout of defense strategies. Finally, the efficient strategy selection approach is designed on the tradeoff between defense cost and benefit. The simulation of attack-defense confrontation in small-scale LAN shows that the proposed approach is reliable and effective.

MSC:
91B06 Decision theory
91A10 Noncooperative games
91A80 Applications of game theory
94A12 Signal theory (characterization, reconstruction, filtering, etc.)

Software:
MulVAL

Full Text: DOI

References:


This reference list is based on information provided by the publisher or from digital mathematics libraries. Its items are heuristically matched to zbMATH identifiers and may contain data conversion errors. It attempts to reflect the references listed in the original paper as accurately as possible without claiming the completeness or perfect precision of the matching.