General Sum Markov Games for Strategic Detection of Advanced Persistent Threats using Moving Target Defense in Cloud Networks

Sailik Sengupta • Subbarao Kambhampati
Ankur Chowdhary • Dijiang Huang

Placing all detection systems in the cloud results in reduced Quality of Service (QoS). Any static placement of detection systems can be easily evaded by an adversary.

Existing MTD for detection system placement do not consider multi-stage attack modeling and assume attacks and detection always succeed. Partial observability hinders scalability.

Markov Game modeling using Attack Graphs. General-sum game because an attacker does not care about defender’s QoS metrics.

Transitions
Use of exploitability score (ES) considers the difficulty of an attack in determining the probability of its success.

Utilities
Use of Impact Score (IS) to determine the impact of attacks.
Use of MiniNET simulations to determine the impact of an IDS on QoS metrics.

Algorithm 1: Dynamic Programming for finding SSE in Markov Games
1. procedure Given (S, M, E, r, U^D, U^K, D = \gamma^S - \gamma^E)
2. OUTPUT V(s), 0 \in ei \in \{A, D\}
3. while i := 1 break
4. // Update Q-values
5. Update Q^P(s, m, e) and Q^A(s, m, e) \forall s \in S, m \in M(s), e \in E(s)
6. using U^P, U^K, and V(s)
7. // Do value and policy computation
8. Calculate V^i(s) and \pi^i(s) for i \in \{A, D\} using the values Q^i(s, m, e)
9. i := i + 1
10. goto loop
11. end procedure

For states further away from the goal, don’t need to monitor at times to enhance performance QoS.

mc-sse(s1) : no-mon: 0.097, mon-LDAP: 0.903
mc-sse(s2) : no-mon: 0.0, mon-Web: 0.539, mon-FTP: 0.461
mc-sse(s3) : pi.no-mon: 0.0, mon-FTP: 1.0

For states closer to the goal, not monitoring is not an option. Security becomes more important that performance.

Emulation on ThoThlab
- Movement strategy is pre-computed.
- SDN used to switch IDS deployments.

This work is supported in part by Naval Research Lab N00173-15-G017, AFOSR grant FA9550-18-1-0067, the NASA grant NNX17AD06G, ONR grants N00014-16-1-2892, N00014-18-1-2442, N00014-18-12840, NSF-USIDOE-1723440, OAC-1642031, SaTC-1528999, 1723440 and NSF-China 61628201 and 61717375. The first author is also supported by an IBM Ph.D. Fellowship.