针对主观攻击者的高级持续安全威胁博弈模型研究

2016年度CCF-启明星辰鸿雁计划终验答辩

院　校 ： 厦门大学通信工程系
答辩人 ： 肖亮 教授

Contents

Part
ONE
第一部分

研究背景

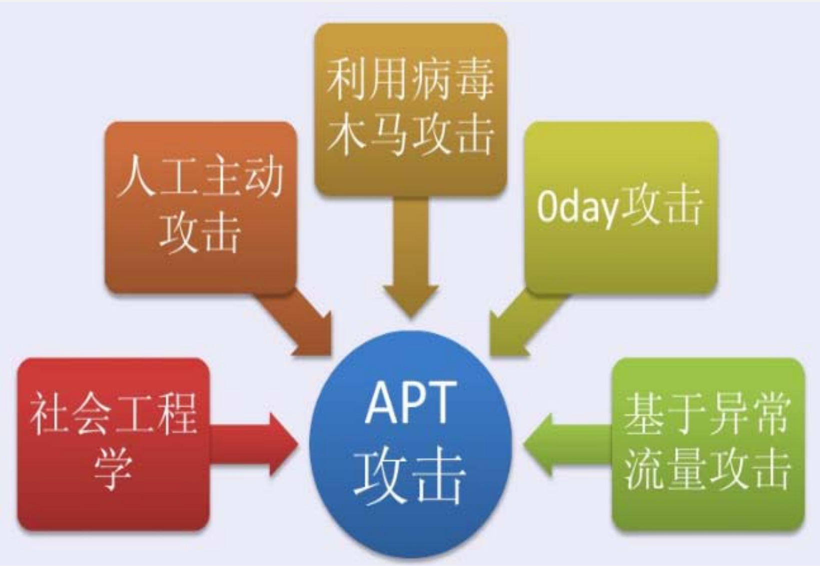
Part ONE

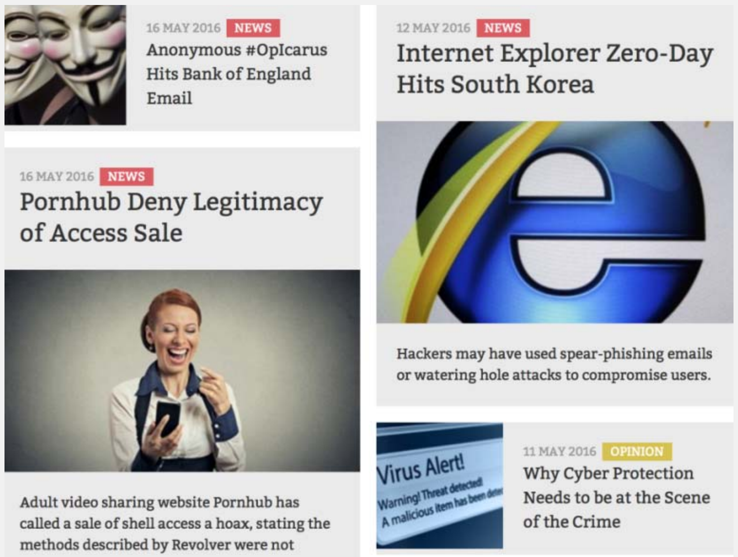
高级持续安全威胁 (APT)

•通过多个步骤入侵网络，避免被检测以长期窃取有价值信息的攻击行为

•特点: 目标明确、持续性、隐蔽性

•意图: 窃取数据而非攻击网络



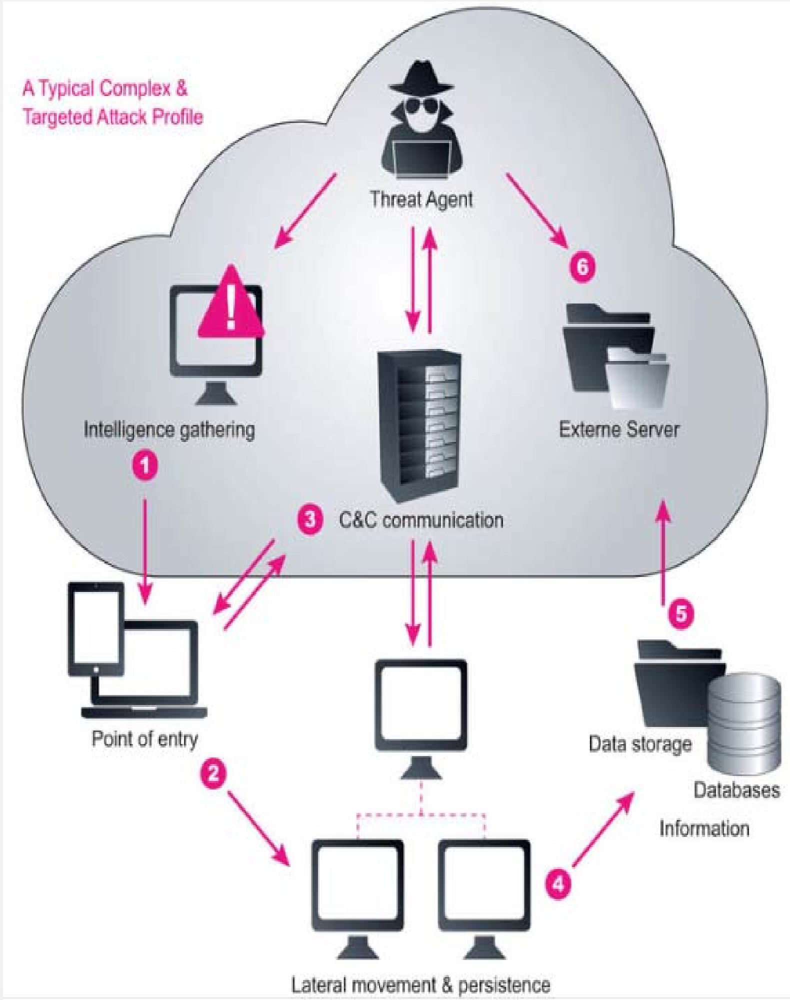


Part ONE

APT攻击模型

•攻击六阶段模型

- 搜集目标系统情报
- 采用恶意代码攻击目标系统
- 利用命令与控制服务器控制目标系统
- 在系统内部横向渗透攻击
- 目标系统的资料发掘，外传
- 掩盖痕迹以长期访问目标系统



Part

TWO

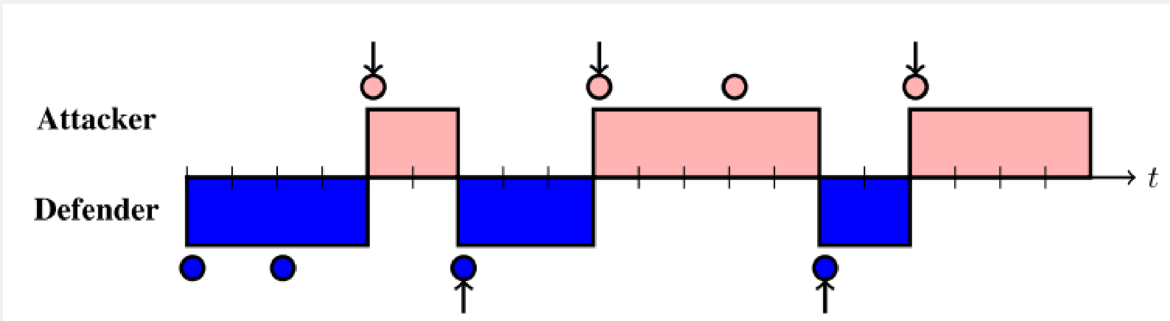
第二部分

理论框架

Part TWO

博弈论

- 博弈论是对 APT 威胁的环境、来源和目标进行建模的重要数学工具
- 现有研究假设攻击者完全理性，选择令其期望收益最大的攻击策略
- 攻击者追求信息或经济收益，决策受主观影响



FlipIt 博弈模型

Part TWO

Allais悖论

High Probability

- ☐ 95% chance to win $10,000
- ☑ 100% chance to win $9,499

0.95*10000>9499

风险规避

Low Probability

- ☑ 5% chance to win $10,000
- ☐ 100% chance to win $501

0.05*10000<501

Gain

风险追求

Lose

风险追求

High Probability

- ☑ 95% chance to lose $10,000
- ☐ 100% chance to lose $9,499

0.95*10000>9499

Low Probability

- ☐ 5% chance to lose $10,000
- ☑ 100% chance to lose $501

0.05*10000<501

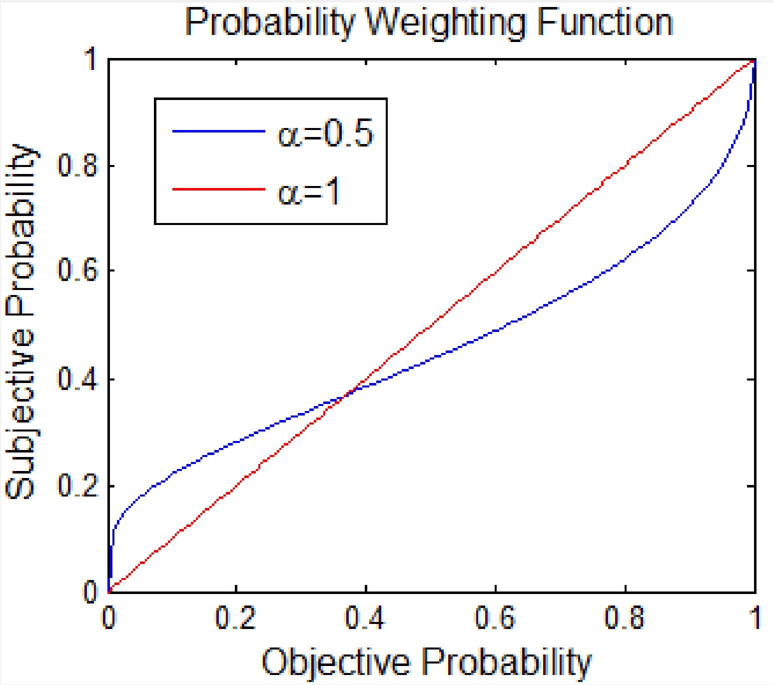
风险规避

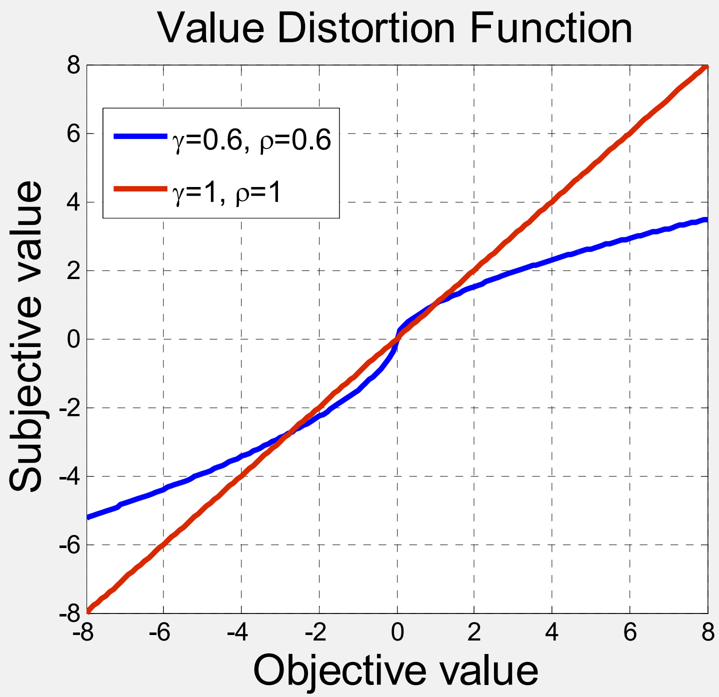
Part TWO

累积前景理论

•概率权重函数：描述主观的攻击者在选择攻击策略时，过于重视小概率的损失，忽视大概率的收益等特征

•价值函数：描述主观攻击者在选择攻击策略时的框架效应，设置参考点衡量相对收益或损失





启明星辰

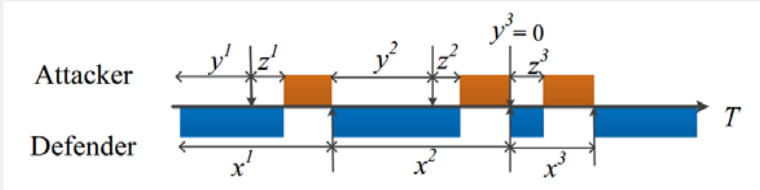
Part
THREE

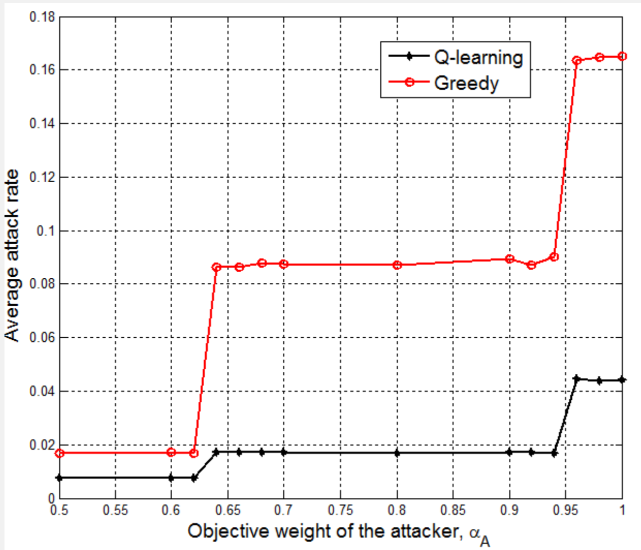
第三部分

研究方法

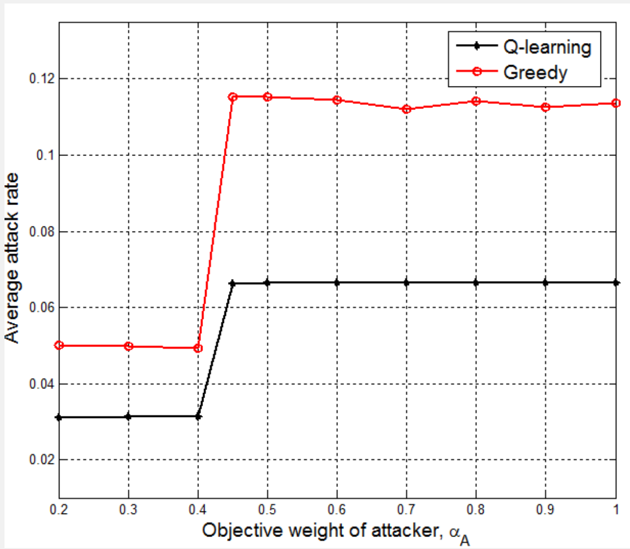
基于前景理论的APT检测方案

- 攻击持续时间和间隔未知
- 研究攻击者主观度对动态纯/混合策略博弈的影响





动态纯策略博弈平均攻击速率



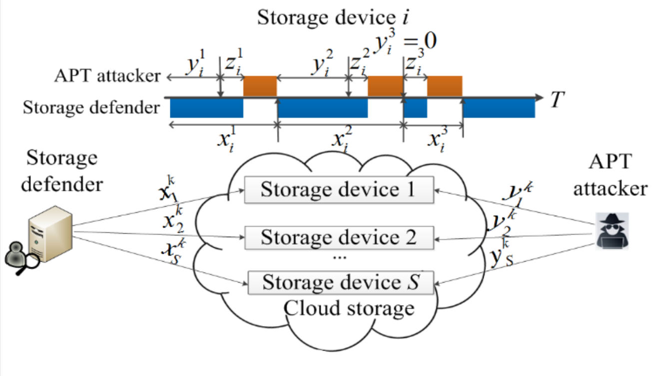
动态混合策略博弈平均攻击速率

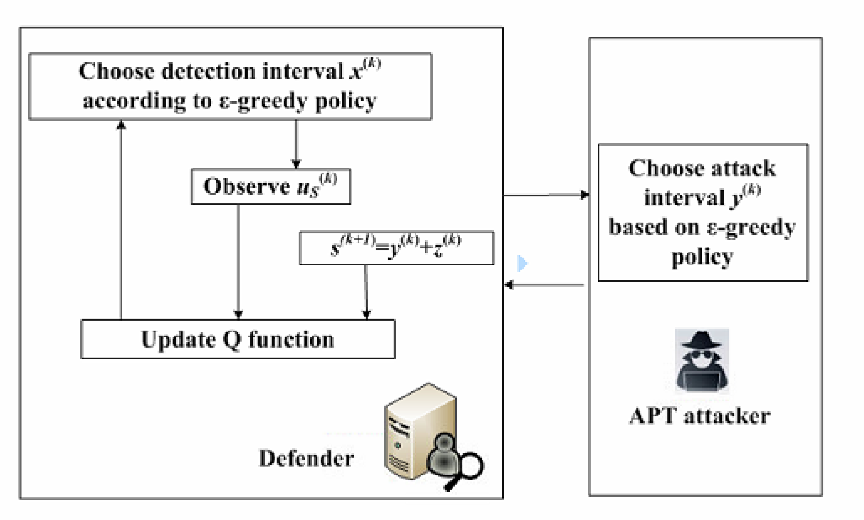
D. Xu, Y. Li, L. Xiao, N. B. Mandayam, and H. V. Poor, "Prospect Theoretic Study of Cloud Storage Defense Against Advanced Persistent Threats," , in Proc. *IEEE Global Communication Conference (GLOBECOM)*, Dec. 2016.

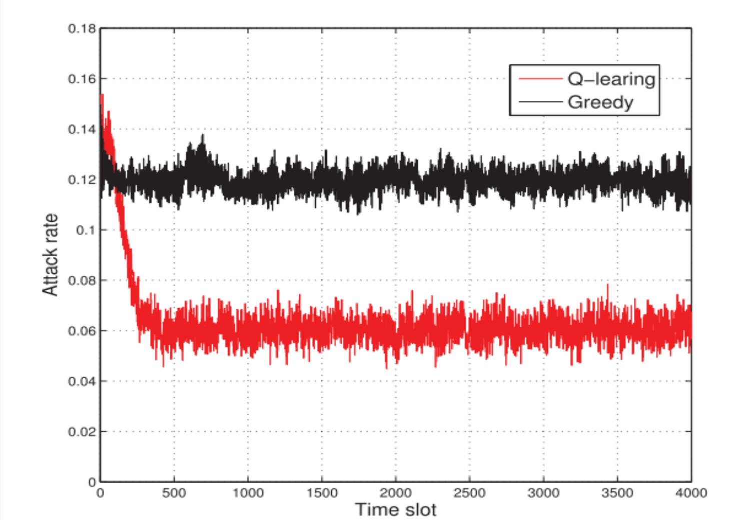
Part THREE

基于前景理论的APT检测方案

- 针对多存储设备，多攻击持续时长的APT攻击模型
- 在未知设备扫描间隔的情况下，利用Q学习获得最佳的防御策略







L. Xiao, D. Xu, C. Xie, N. B. Mandayam, and H. V. Poor, "Cloud Storage Defense Against Advanced Persistent Threats: A Prospect Theoretic Study," *IEEE Journal on Selected Areas in Communications*, Mar. 2017.

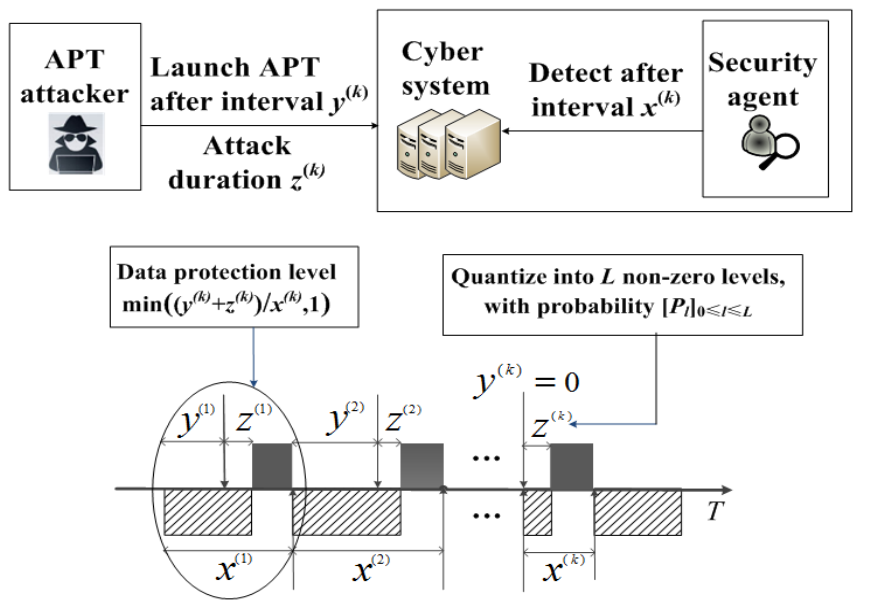
一种云存储系统的持续性攻击的检测方法，中国，发明专利， 201710018243.1，2017年5月3日

Part THREE

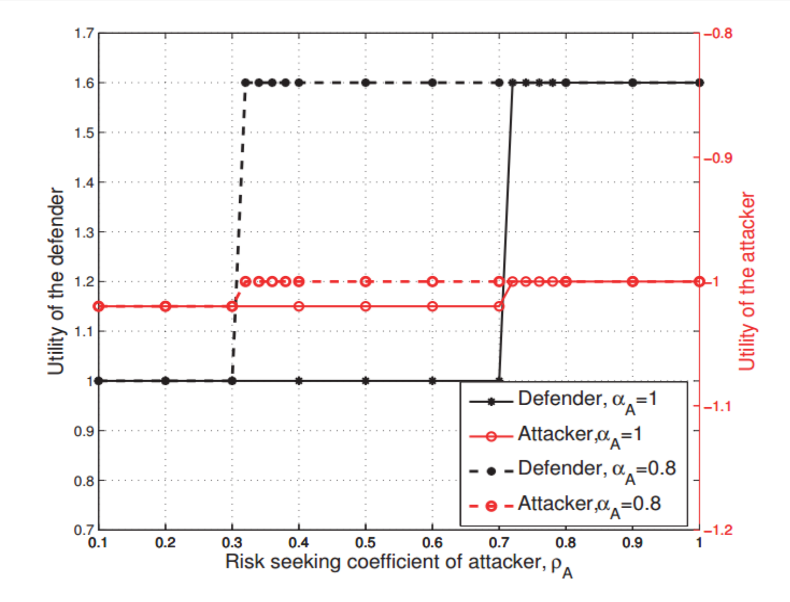
基于累积前景理论的APT检测方案

•结合APT攻击的框架效应研究APT攻防方案

•引入累积前景理论研究多输出的系统模型



APT检测博弈模型



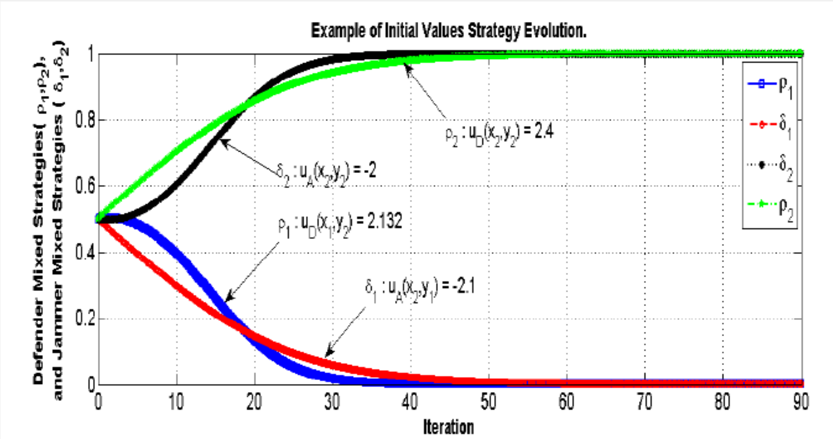
NE结果图

D. Xu, L. Xiao, N. B. Mandayam, H. V. Poor, "Cumulative Prospect Theoretic Study of a Cloud Storage Defense Game Against Advanced Persistent Threats," in Proc. *IEEE International Conference on Computer Communications (INFOCOM WKSHPS), -BigSecurity*, May 2017.

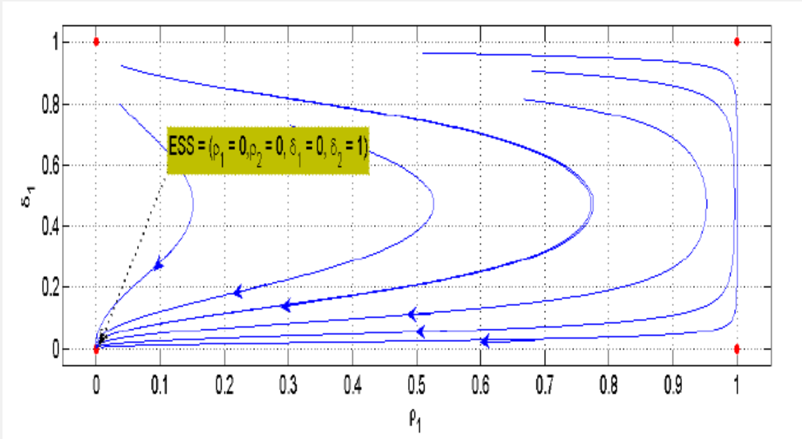
Part THREE

基于演化博弈论的APT防御机制

- 利用演化博弈理论捕捉云端APT长期持续性的攻击行为
- 利用演化稳定策略检测防御机制的纳什均衡能否抵抗轻微的扰动



概率演化



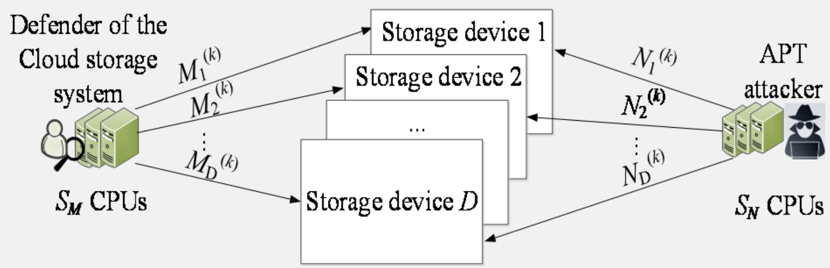
相位图

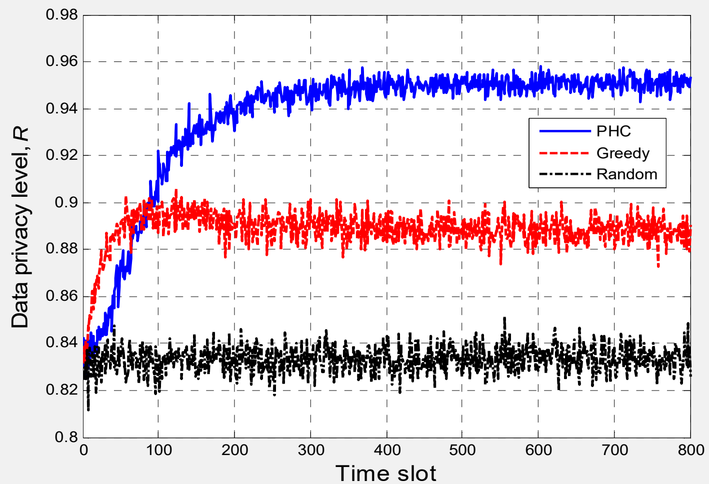
A. Abass, L. Xiao, N. B. Mandayam, and Z. Gaijic, "Evolutionary Game Theoretic Analysis of Advanced Persistent Threats Against Cloud Storage," *IEEE Access*, Apr. 2017.

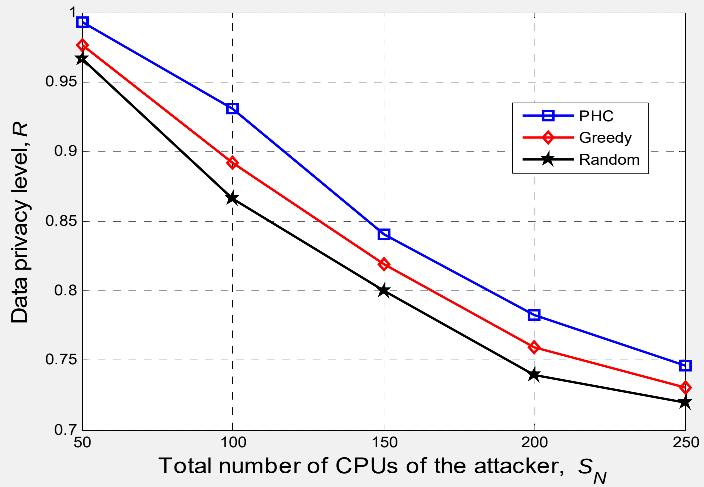
Part THREE

基于CBG的APT防御博弈

- 动态云储存环境下获取检测APT攻击的最优检测资源分配
- 防御系统选择用于安全检测的CPU资源个数M



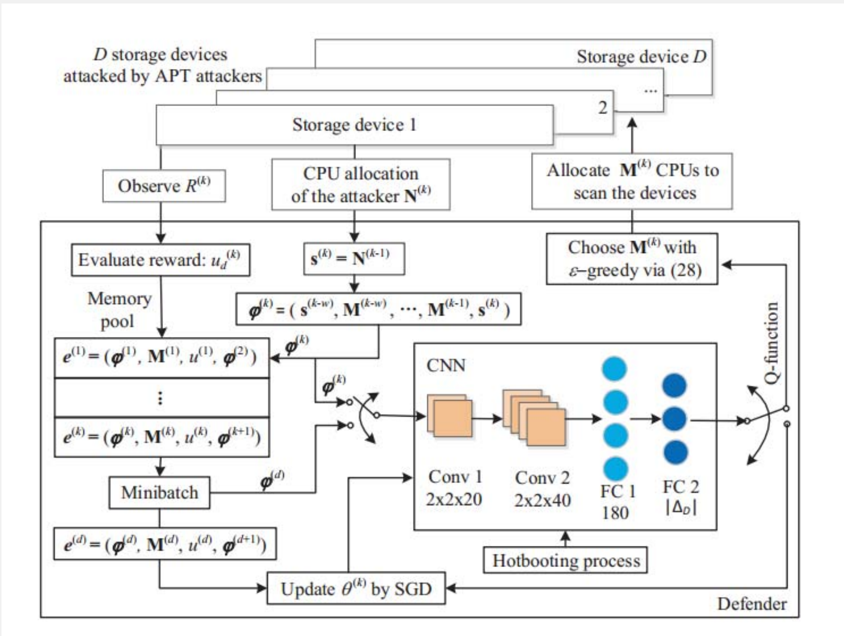




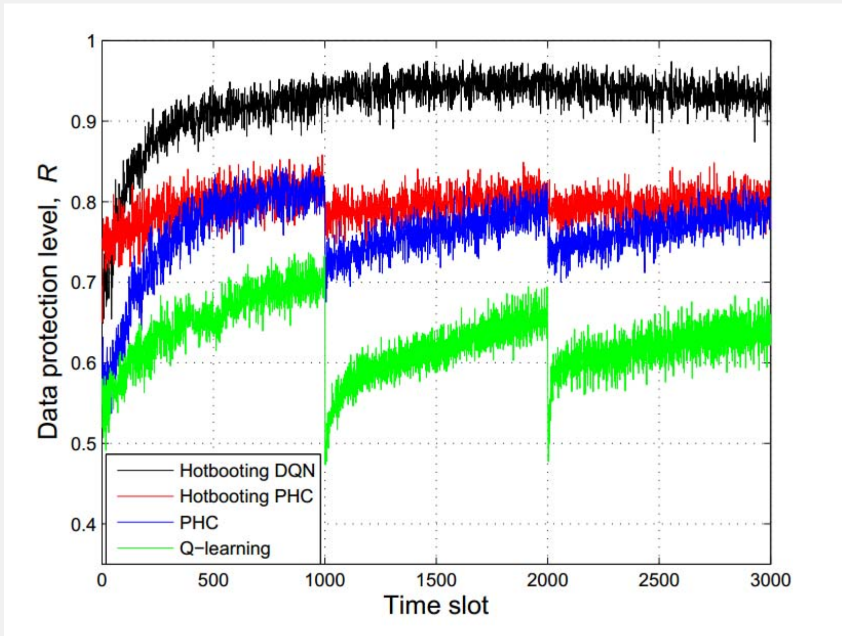
M. Min, L. Xiao, C. Xie, M. Hajimirsadeghi, N. B. Mandayam, "Defense Against Advanced Persistent Threats: A Colonel Blotto Game Approach," in Proc. *IEEE International Conference on Communications (ICC)*, May 2017.

基于CBG的APT防御博弈

- 研究在时变的数据存储模型下的APT攻击策略
- 利用深度强化学习提高学习速率，增强系统防御能力



基于DQN的APT防御策略



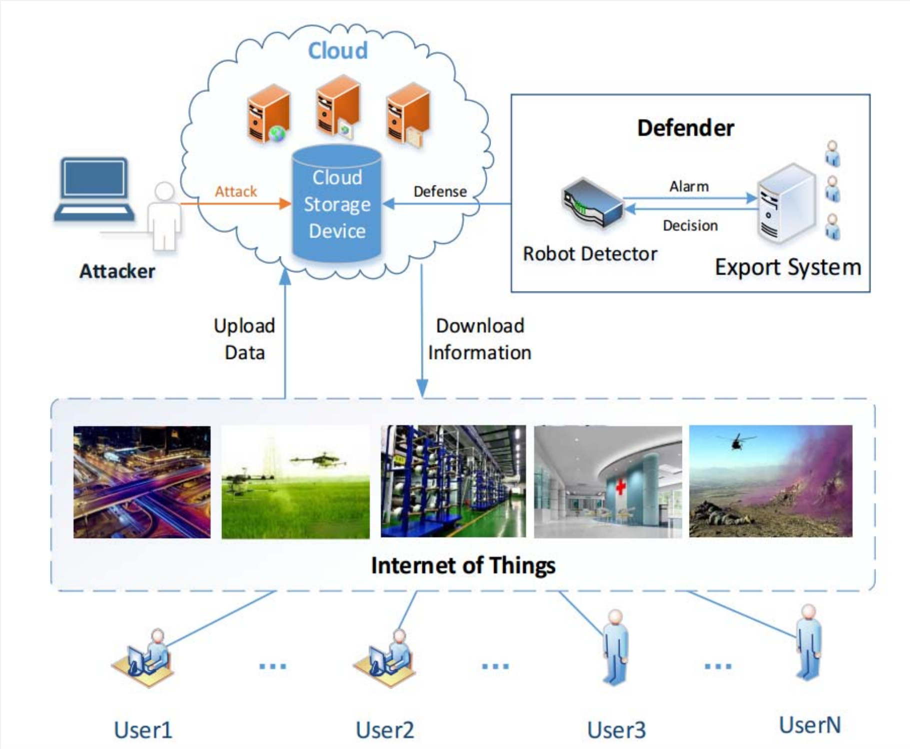
算法性能比较

M. Min, L. Xiao, C. Xie, M. Hajimirsadeghi, N. B. Mandayam, "Defense Against Advanced Persistent Threats in Dynamic Cloud Storage: A Colonel Blotto Game Approach", *IEEE Internet of Things Journal*, under review.
基于强化学习的检测高级持续威胁的资源调度方法，中国，发明专利，201710684939.8, 2017年8月11日

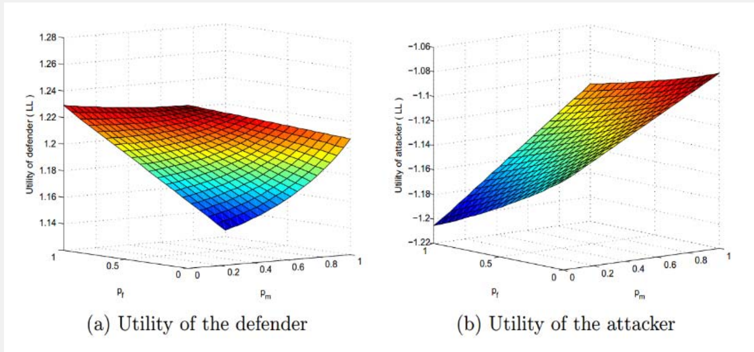
Part THREE

基于专家系统的APT防御机制

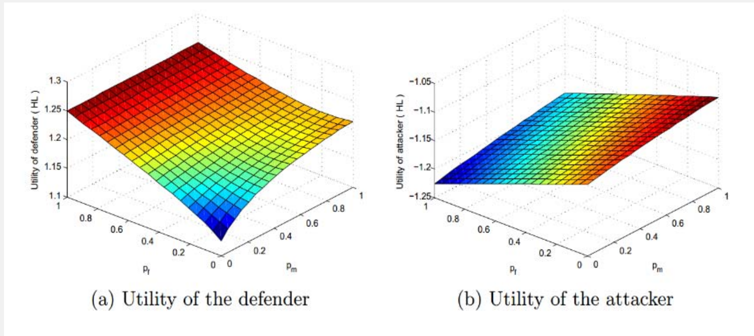
- 专家系统：监督系统，根据虚警率和漏报率做出决策



APT防御模型



低APT攻击水平



高APT攻击水平

Q. HU, S. Lv, Z. Shi, L. Sun and L. Xiao, " Defense Against Advanced Persistent Threats with Expert System for Internet of Things, " in Proc. *IEEE/IFIP International Conference on Wireless Algorithms, Systems, and Application*, June 2017.

论文、专利发表情况

1. Cloud Storage Defense Against Advanced Persistent Threats: A Prospect Theoretic Study, *IEEE Journal on Selected Areas in Communications*, 35(3), 534-544.
2. Evolutionary Game Theoretic Analysis of Advanced Persistent Threats Against Cloud Storage, *IEEE Access*, 5, 8482-8491.
3. Physical-Layer Authentication Based on Extreme Learning Machine, *IEEE Communication Letters*, 35(3), 1089-7798.
4. Cloud-based Malware Detection Game for Mobile Device with Offloading, *IEEE Transactions on Mobile Computing*, 16(10), 2742 - 2750.
5. Attacker-Centric View of a Detection Game Against Advanced Persistent Threats, *IEEE Transactions on Mobile Computing*, under review
6. Defense Against Advanced Persistent Threats in Dynamic Cloud Storage: A Colonel Blotto Game Approach, *IEEE Internet of Things Journal*, under review
7. Two-Dimensional Anti-Jamming Communication Based on Deep Reinforcement Learning, *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, Mar. 2017.
8. Game Theoretic Study of Protecting MIMO Transmission Against Smart Attacks, *IEEE International Conference on Communications (ICC)*, May 2017. (Best paper award)
9. Phy-layer Authentication with Multiple Landmarks with Reduced Communication Overhead, *IEEE International Conference on Communications (ICC)*, May 2017.

Part THREE

论文、专利发表情况

10. Defense Against Advanced Persistent Threats: A Colonel Blotto Game Approach, *IEEE International Conference on Communications (ICC)*, May 2017.
11. Cumulative Prospect Theoretic Study of a Cloud Storage Defense Game Against Advanced Persistent Threats, *IEEE International Conference on Computer Communications (INFOCOM WKSHPS), -BigSecurity*, May 2017.
12. FuzzyDP: Fuzzy-based Big Data Publising Aginst Inquiry Attacks, *IEEE Conference on Computer Communication Workshops (INFOCOM WKSHPS), - MobiSec*, May 2017.
13. Energy Trading Game for Microgrids Using Reinforcement Learning, *EAI International Conference on Game Theory for Network*, May 2017. (Best paper award)
14. Defense Against Advanced Persistent Threats with Expert System for Internet of Things, *IEEE/IFIP International Conference on Wireless Algorithms*, Systems, and Application, June 2017.
15. Reinforcement Learning Based Mobile Offloading for Cloud-based Malware Detection, *IEEE Global Communication Conference (GLOBECOM)*, Dec. 2017.
16. Anti-Jamming Communication Game for UAV-aided VANETs, *IEEE Global Communication Conference (GLOBECOM)*, Dec. 2017.
17. 一种云存储系统的持续性攻击的检测方法，中国，发明专利， 201710018243.1，2017年5月3日
18. 基于强化学习的检测高级持续威胁的资源调度方法，中国，发明专利，201710684939.8, 2017年8月11日

CCF-Venustech

THANKS!

谢 谢 观 看

lxiao@xmu.edu.cn