Mobile Offloading for Cloud-based Malware Detections with Learning

Liang Xiao       Yanda Li

厦门大学

中山大学       广州

NOV. 23, 2016
Outline

• Background & motivation
• Cloud-based malware detection for mobile devices:
  • Challenges & opportunities by big data
• Nash equilibrium (NE) of the cloud-based malware detection game:
  • Competition & cooperation among mobile devices
• Reinforcement learning based cloud malware detection
• Conclusions
Motivation

- Malware: Viruses, trojans, spywares and other intrusive codes
- Aim to disrupt operations, access private information, display unwanted advertising, etc
- Hummingbad malware that generates fake clicks for adverts infected 10 million Android smartphones and made $300,000/month for the attacker
- The average smartphone infection rate increased 96% in the first half of 2016, compared to the second half of 2015
Big Data in Malware Detections

- In 2015, 144 million new malwares were found: 274 new unknown malware were produced and launched in every minute.
- The number of Android malware samples in Nokia malware database increased by 75% in the first half of 2016.
Malware Detections

- Signature-based detection: Identify malwares by their signatures
  - Rely on human expertise in creating labels for malicious behaviors
  - Low computational complexity and low false alarm rate
  - Vulnerable to zero-day attacks

- Anomaly-based detection: Use the knowledge of normal behavior
  - Detect new malwares
  - Large sample size required in the training phase
  - High computation complexity & high false alarm rate

- Hybrid detection: Signature-based + anomaly-based detection techniques
Malware Detection at Mobile Devices

- Big data in malware detection: A large number of traces generated by the applications run at a mobile device
- Challenges:
  - High storage cost
  - Long detection delay
  - Zero-day malware attacks: Attack signatures not downloaded in time
- Benefits: Detection accuracy depends on the size of the virus database downloaded from security servers

117903 lines of log data

- Size of the whole operation data
- Size of the generated log data

The log data evaluated in Norton security application
Cloud-based Malware Detection System

- Behavior-based malware detection system: k-means clustering [Iker’11]
- Online cloud anomaly detection: SVM [Watson’16]

**Advantages:**
- Fast computation to run more advanced and complex detection algorithms
- More accurate detection with a large-size signature database
- Address zero-day vulnerabilities
Mobile Offloading in the Malware Detection

- Cloud-based malware detection vs. local detection
  - Transmission delay, computation speed, detection accuracy, storage cost
- User competition vs. cooperation in the malware detection
  - Compete for the limited network bandwidth
  - Contribute the malware signature database to improve the malware detection accuracy at the cloud

Mobile device
- CPU speed
- Storage of log data
- Data privacy
- Energy

AP/BS
- Connectivity technology (4G/3G/Wi-Fi)
- Time-varying radio bandwidth
- Queue delay
- Transmission cost

Cloud
- Powerful computation
- Large-size malware database
- Runtime detection
- Request delay
Mobile Offloading Game

\[
\begin{align*}
&\text{Cloud computation capacity} \\
&\text{Unit transmission cost} \\
&\text{Amount of app traces} \\
&\text{Accuracy coefficient}
\end{align*}
\]

\[
u_i(x_i, x_{-i}) = \left( \frac{R}{\sum_{m=1}^{M} x_m C_m} - \frac{\omega}{b_i} \right) x_i C_i + \gamma \sum_{m=1}^{M} x_m C_m
\]

Offloading rate
**Static Cloud-based Detection Game**

- NE of the static game: No mobile station can benefit by unilaterally leaving the NE strategy \( u_i(x_i^*, x_{-i}^*) \geq u_i(x_i, x_{-i}^*), \forall x_{-i}^* \)

\[
x_i^* = \begin{cases} 
0, & \text{if } \frac{Rb_i}{\omega - \gamma b_i} < \sum_{m \neq i} x_mC_m \\
1, & \left( \sum_{m \neq i} x_mC_m \right)^2 + \left( 2C_i - \frac{Rb_i}{\omega - \gamma b_i} \right) \sum_{m \neq i} x_mC_m + C_i^2 < 0 \\
\frac{1}{C_i} \left( \sqrt{\frac{Rb_i \sum_{m \neq i} x_mC_m}{\omega - \gamma b_i}} - \sum_{m \neq i} x_mC_m \right), & \text{otherwise,}
\end{cases}
\]

Severe shadow fading

Light communication overhead
Detection Performance at the NE

Cloud computation resource = 1 Gbps
Trace generation speed = 1 Mbps
Transmission cost factor = 0.2
Accuracy coefficient = 0.5
Dynamic Malware Detection Game

- Dynamic cloud-based malware detection game: Repeated interactions among mobile devices in time-variant network environments
- Q-learning based malware detection: Offloading rate is chosen without knowing the network model and the app trace generation model
- A model-free reinforcement learning algorithm for an agent to derive the optimal strategy via trial-and-errors in a dynamic game
Q-Learning Based Malware Detection

- **State**: Network bandwidth and the offloading rates of the other mobile devices at last time, \( s_i^k = [x_{i-1}^k, b_i^k] \)

- **Q-function**: Estimated discounted long-term utility for each state-action pair
  - Update via iterative Bellman equation:

\[
Q(s^k, x^k) \leftarrow (1 - \gamma)Q(s^k, x^k) + \gamma (u_i(s^k, x^k) + \delta \max_{\mu \in \mathcal{X}} Q(s^{k+1}, \mu))
\]

  - Learning rate: Weigh the current Q-function
  - Discount factor: Uncertain future reward

- **Encourage exploration with \( \varepsilon \)-greedy policy**: Not trapped in the local optimum at the beginning of the game
Q-Learning Based Offloading in Malware Detections

Mobile device

App traces
generation $C$

Divide APP traces

Q-learning offloading rate $\epsilon^k$ select based $\epsilon$-greedy policy

$\epsilon^k C$ APP traces

Cloud server

Machine learning based malware detection

Apps feature extraction

Detection result

AP/BS
Simulation Results

Cloud computation resource = 8 Gbps
Trace generation speed = 1 Mbps
Transmission cost factor = 0.1
Accuracy coefficient = 0.8
Radio bandwidth $\in \{1/6, 1/5, 1/4\} \times 10\text{MHz}$
Average Performance

[Xiao, Li, INFOCOM –BigSecurity’15]
Conclusion

- We formulated a cloud-based malware detection game and provided the NE of the game to investigate the user cooperation and competition.
- A Q-learning based malware detection strategy was proposed in the dynamic game with time-variant radio networks.
  - Reduce the detection delay of mobile users by 33%.
  - Increase the detection accuracy gain by 40%.
- Further work:
  - Improve the cloud-based malware detection game model.
  - Improve the performance of the Q-learning based malware detection with deep learning and data mining in dynamic environments.
  - Build prototype and evaluate the performance via experiments.
Questions?

lxiao@xmu.edu.cn