# IPS.3: Reinforcement Learning Based Mobile Offloading for Cloud-based Malware Detection

Xiaoyue Wan, Geyi Sheng, Yanda Li, Liang Xiao, Xiaojiang Du

Speaker: Geyi Sheng
Dept. of Communication Engineering, Xiamen University
Xiamen Fujian, China

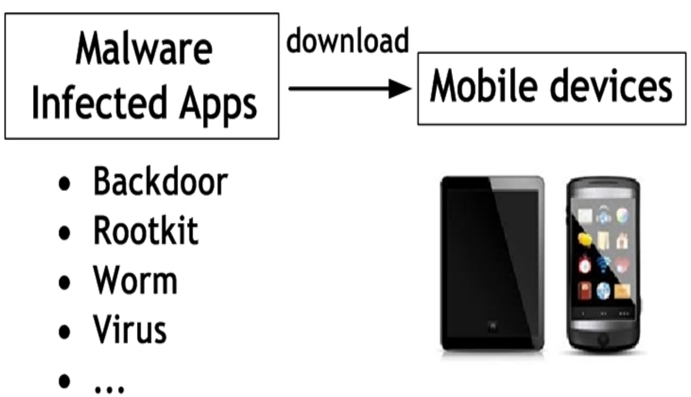
Dec. 7, 2017

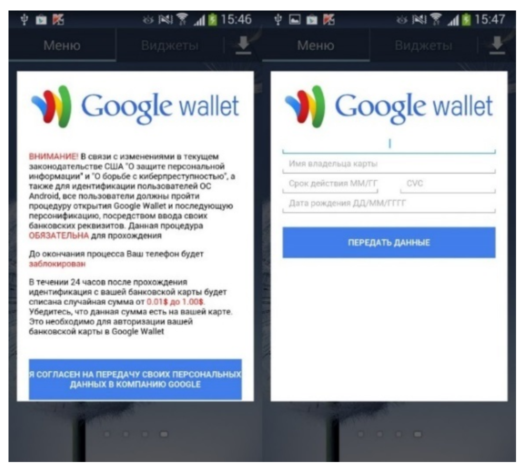
# Outline

- Background & motivation
  - Challenges & opportunities from big data
- Cloud-based malware detection model for mobile devices
- Learning based malware detection schemes
  - Hotbooting-Q based malware detection
  - DQN-based malware detection
- Simulation results
- Conclusion

# Motivation

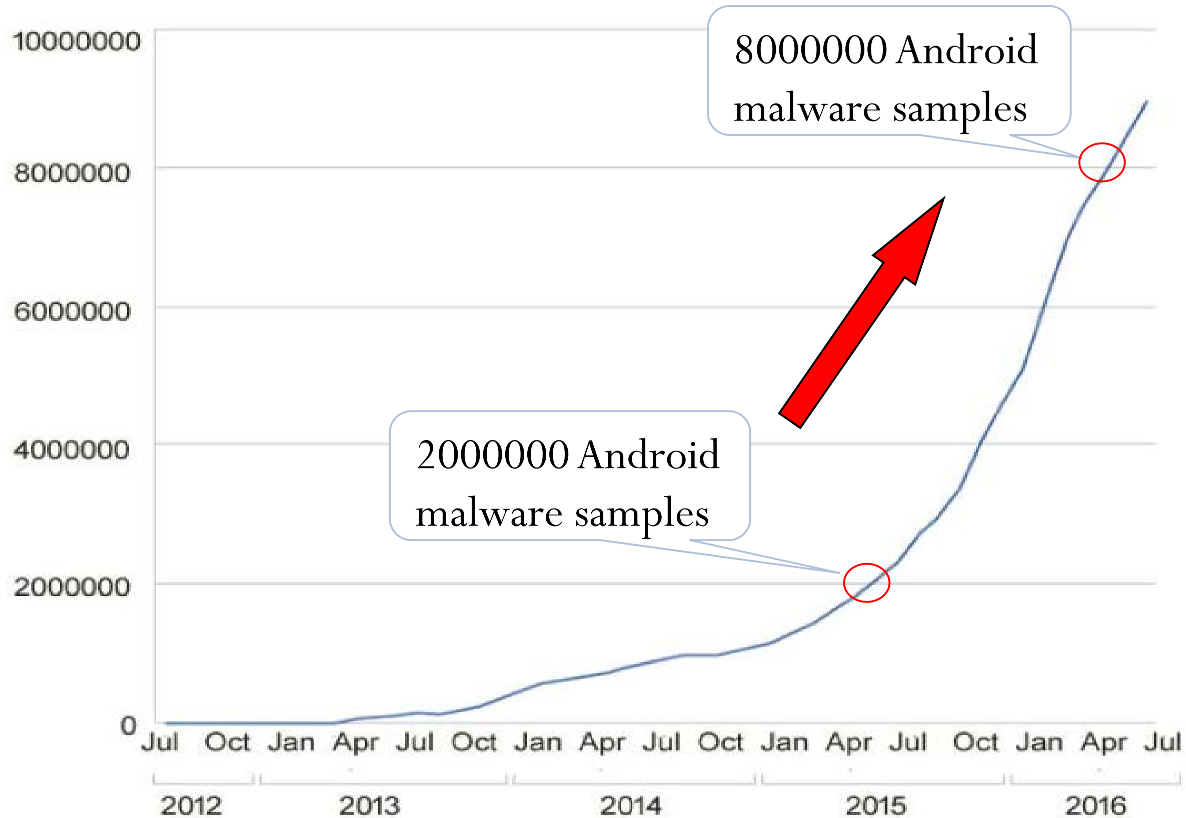
- Malware refers to viruses, Trojans, spywares and other intrusive code
  - Used to disrupt computer or mobile operations, gather sensitive information, gain access to private computer systems, or display unwanted advertising [Idika'07]
- The average smartphone infection rate increased 96 percent in the first half of 2016, compared to the second half of 2015 [Nokia'16]
  - Up to 10 million Android smartphones around the world have been infected by Hummingbad malware that generates fake clicks for adverts, which makes 300,000$ per mon for the malware attacker [BBC'16]




# Big Data in Malware Detection

- In 2015, about 144 million new malwares were found, in which 274 new unknown malware were produced and launched every minute [Check-Point'16]
- The number of Android malware samples in Nokia malware database increased by 75 percent in the first half of 2016 [Nokia'16]
- Number of Android malware samples in Nokia malware

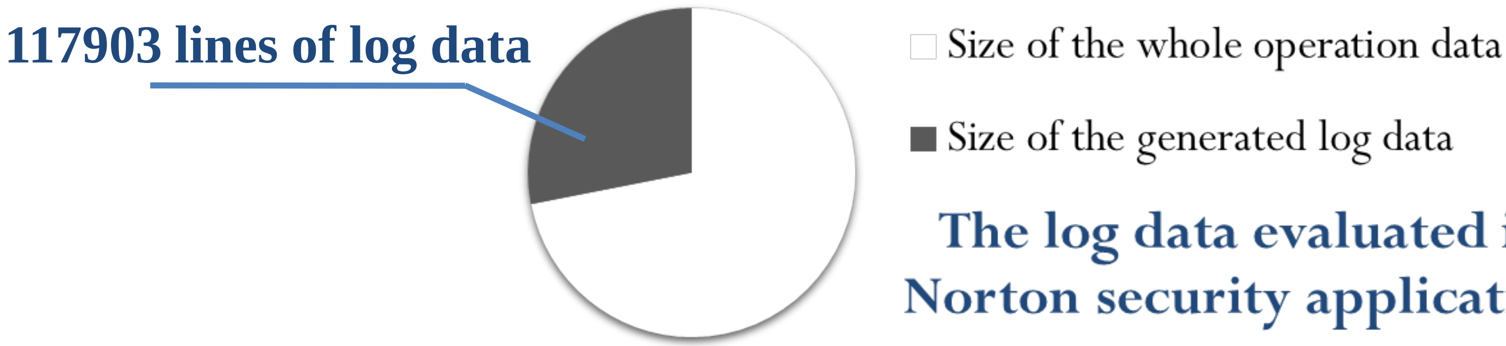


# Malware Detection Methods

- Signature-based detection
  - Rely on human expertise in creating the label of malicious behaviors
  - Applicable for light computation on smartphones
  - Fail to address zero-day malware: an attack not publicly reported or announced before becoming active
- Anomaly-based detection
  - Applicable to address various types of malwares
  - A large volume of samples required in the training phase
  - High computation complexity & high false alarm rate
- Hybrid detection
  - Raise detection rates of known malwares
  - Decrease the false positive rate for unknown attacks

# Challenges of Malware Detection at Smartphones

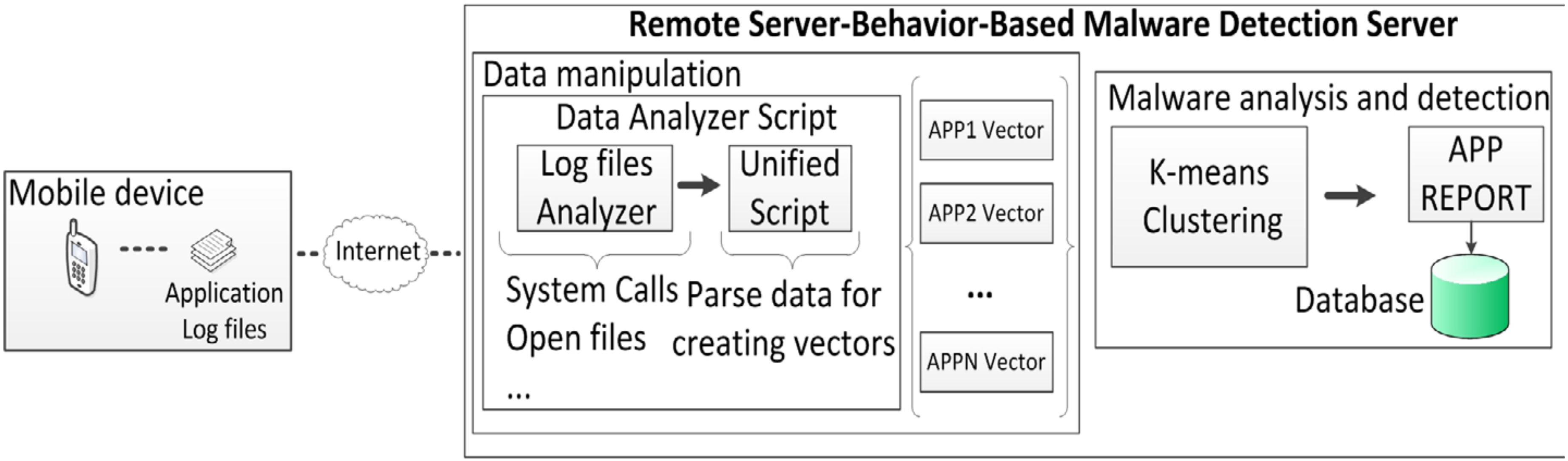
- Big app trace data: A large number of log data is generated by the applications run at smartphone
  - High storage cost
  - Limited computational speed to run the detection algorithm
  - Detection accuracy limited by the size of the virus database at the smartphone downloaded from the security servers
  - Zero-day malware attacks




**The log data evaluated in Norton security application**

# Cloud-based Malware Detection System

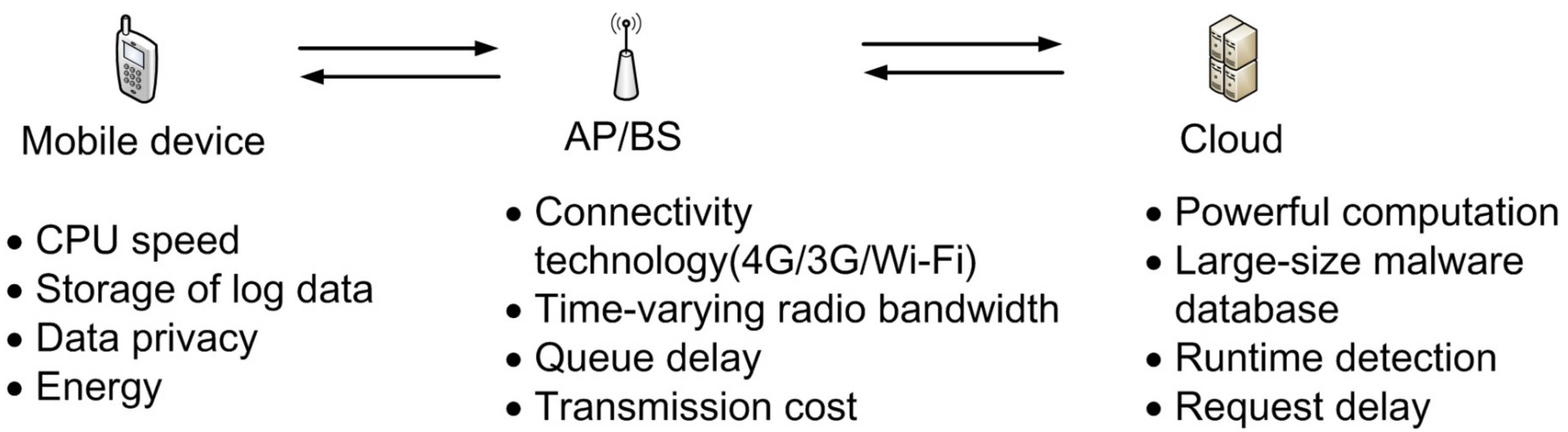
- Online cloud anomaly detection for both system and network level data using dedicated monitoring components based on SVM [Watson'16]




- Advantages of cloud-based detection:
  - 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 Cloud-based Malware Detection

- Smartphone divides real-time app traces and labels with serial numbers
  - Offload a portion of the traces to the cloud for malware
- Cloud-based detection vs. local detection
  - Transmission delay, CPU occupying, detection accuracy, storage cost
- Mobile users in the malware detection
  - compete for the cloud computational resource and the network bandwidth, and cooperate to improve the malware detection accuracy at the cloud

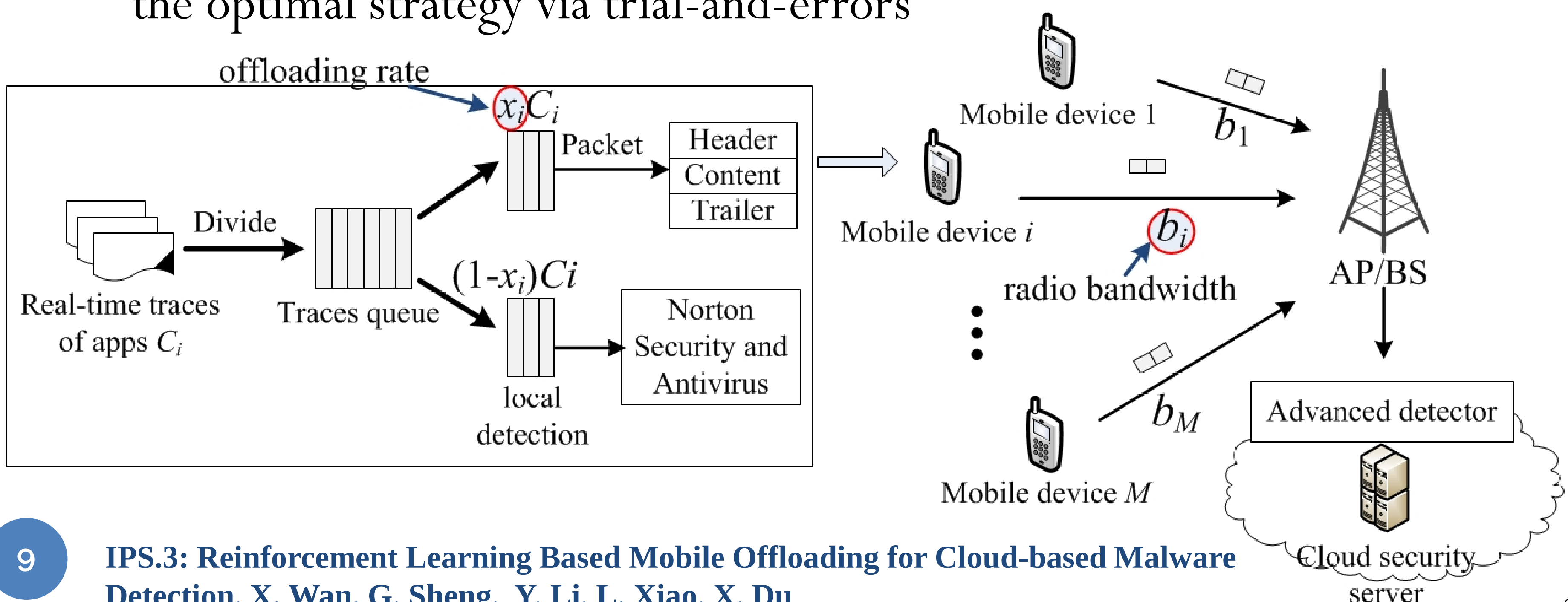





**IPS.3: Reinforcement Learning Based Mobile Offloading for Cloud-based Malware Detection, X. Wan, G. Sheng, Y. Li, L. Xiao, X. Du**

# Mobile Offloading Model

- Repeated interactions among mobile devices in the cloud-based malware detection under time-variant network environment
- Q-learning based malware detection: Offloading rate is chosen without knowing the network bandwidth 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

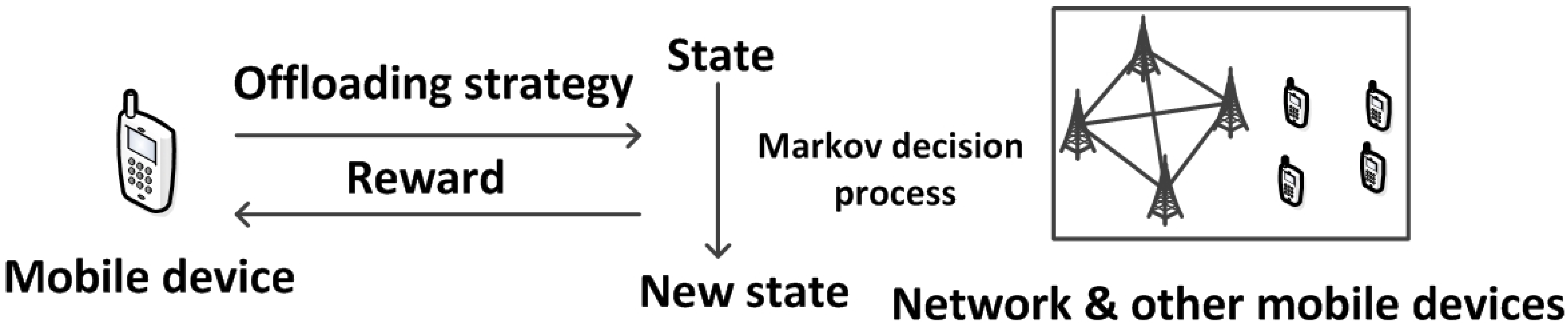





**IPS.3: Reinforcement Learning Based Mobile Offloading for Cloud-based Malware Detection, X. Wan, G. Sheng, Y. Li, L. Xiao, X. Du**

# Q-Learning based Malware Detection

- State: Network bandwidth and the offloading rates of the other devices at last time
- Q-function: Estimated discounted long-term utility for each state-action pair
- Q-function update based on iterative Bellman equation: Estimate of optimal future value
- Encourage exploration with ε-greedy policy: Avoid tracking in the local optimum at the beginning

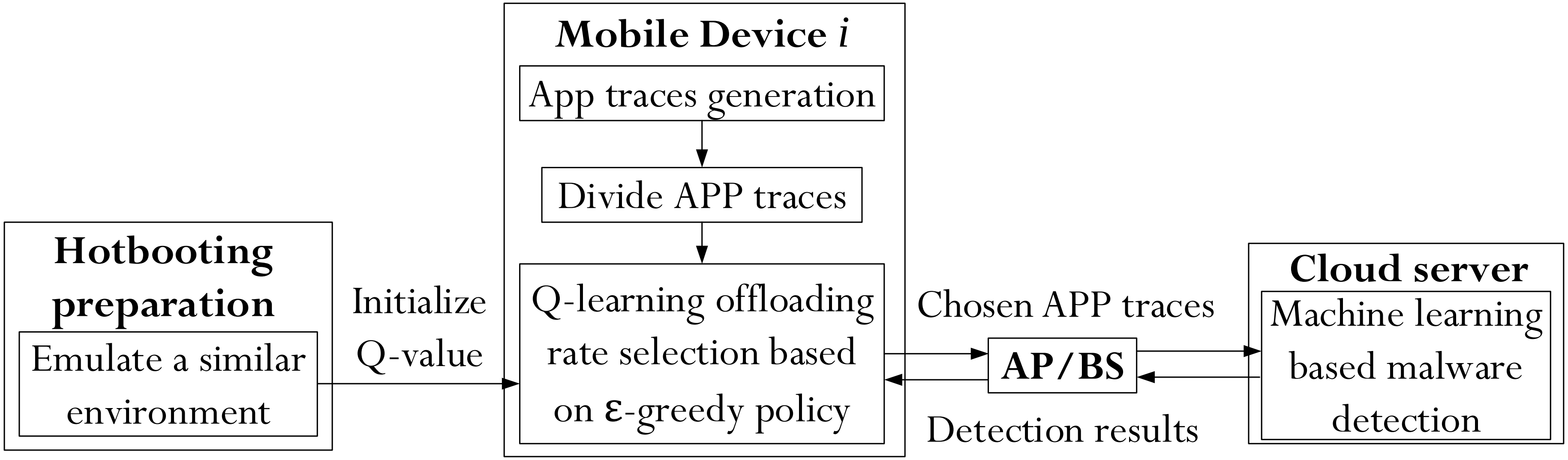




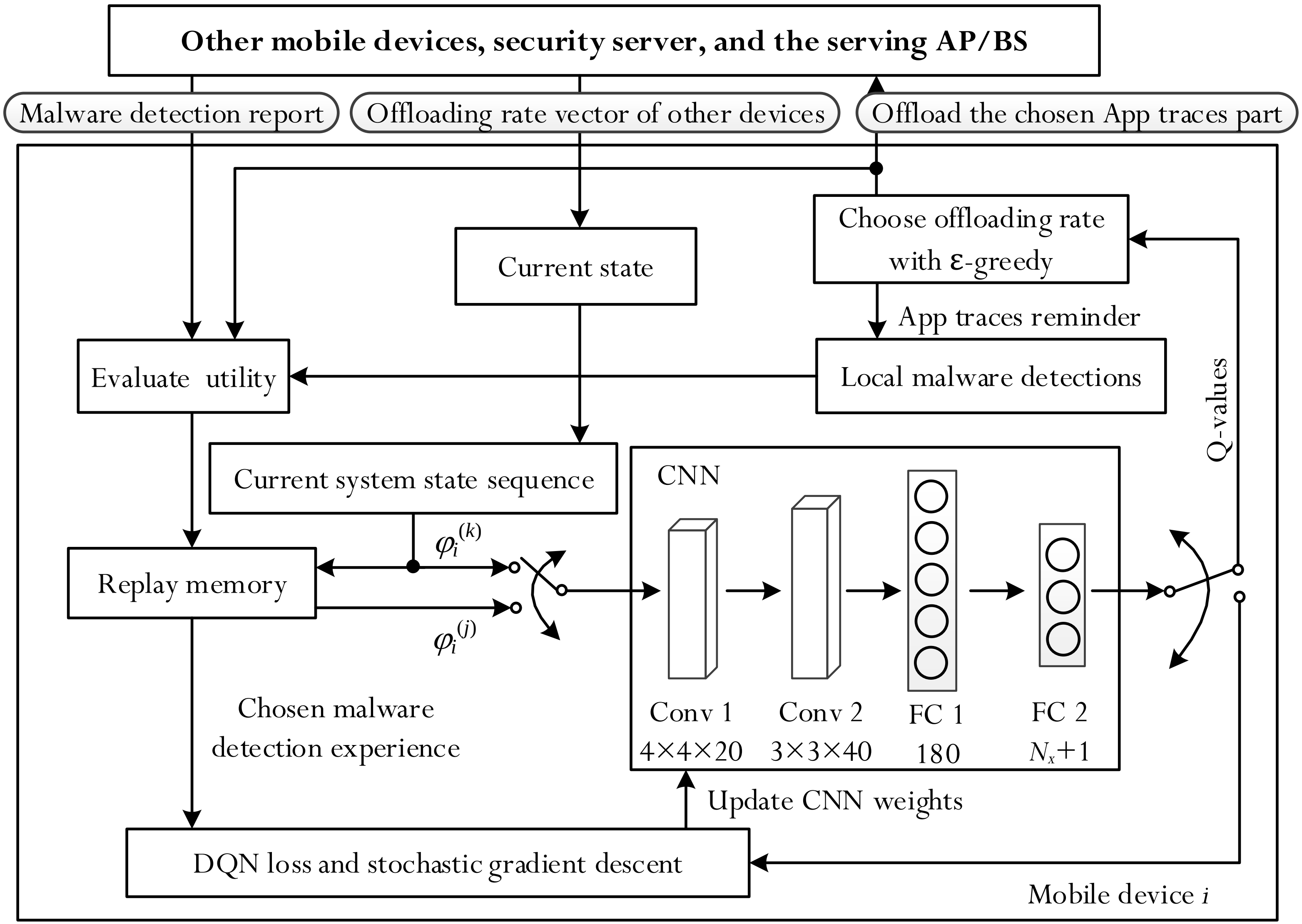

IPS.3: Reinforcement Learning Based Mobile Offloading for Cloud-based Malware Detection, X. Wan, G. Sheng, Y. Li, L. Xiao, X. Du

# Hotbooting Q-learning based Malware Detection

- Hotbooting technique that initializes the Q-value based on the training data in similar scenarios
  - Decrease the random explorations at the beginning
  - Accelerate the learning speed in the dynamic game



# DQN-based Malware Detection






IPS.3: Reinforcement Learning Based Mobile Offloading for Cloud-based Malware Detection, X. Wan, G. Sheng, Y. Li, L. Xiao, X. Du

# Simulation Results

- Setup:

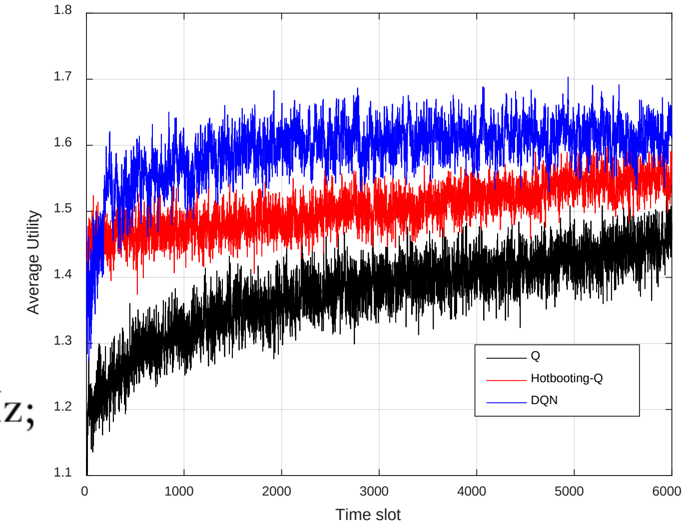
Cloud computation resource= 1Gbps ;

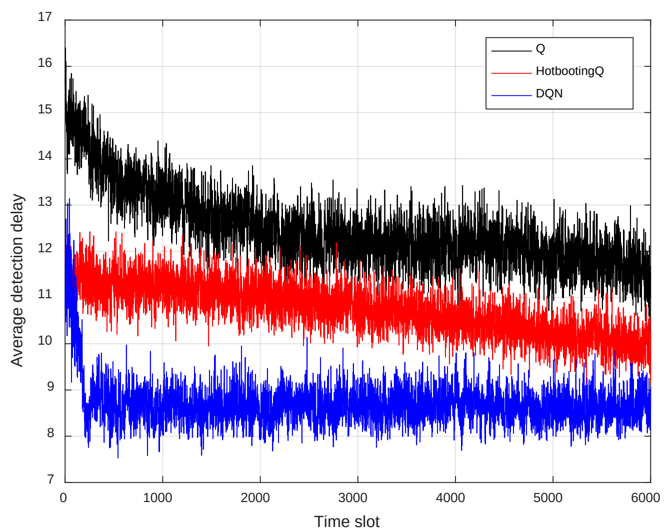
Transmission cost factor= 0.1;

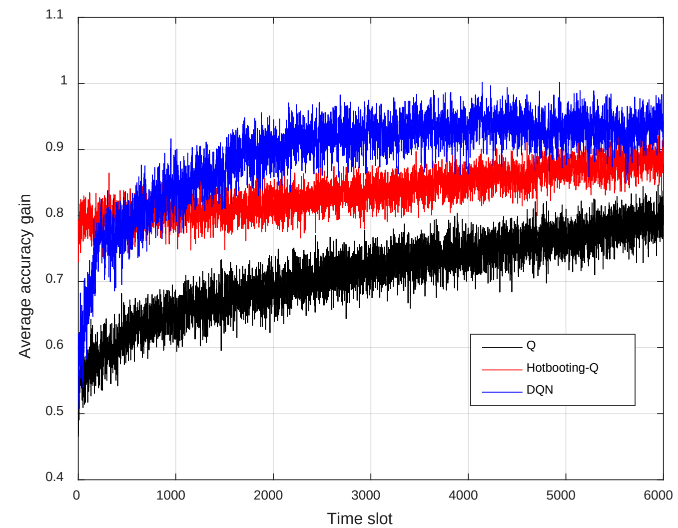
Accuracy coefficient= 1.5;

Number of mobile devices= 2;

Transmission bandwidth $\in \{\frac{1}{7},\frac{1}{6},\frac{1}{5},\frac{1}{4},\frac{1}{3}\}\times$10MHz; or $\in \{\frac{1}{10},\frac{1}{9},\frac{1}{8},\frac{1}{7},\frac{1}{6}\}\times$10MHz.






**IPS.3: Reinforcement Learning Based Mobile Offloading for Cloud-based Malware Detection, X. Wan, G. Sheng, Y. Li, L. Xiao, X. Du**

# Conclusion

- We have formulated a cloud-based malware detection model, in which the mobile devices compete for the limited radio transmission resource and cooperate to improve the malware detection accuracy of the security server.
- A hotbooting-Q based mobile offloading strategy has been proposed to improve the malware detection performance compared to the Q-learning based scheme, and the performance is further improved by the DQN-based malware detection.

Questions?

[*lxiao@xmu.edu.cn*](mailto:lxiao@xmu.edu.cn)