SDN-Supported Collaborative Approach for DDoS Flooding Detection and Containment

Tommy Chin Jr., Kaiqi Xiong • Department of Computing Security • Rochester Institute of Technology • {txc9627,kxxics}@rit.edu
Xenia Mountrouidou • Department of Computing Science • Jacksonville University • xmountr@ju.edu
Xiangyang Li • Information Security Institute • Johns Hopkins University • xyli@jhu.edu

GENI Engineering Conference 22 and US Ignite Application Summit
March 2015
Washington, DC

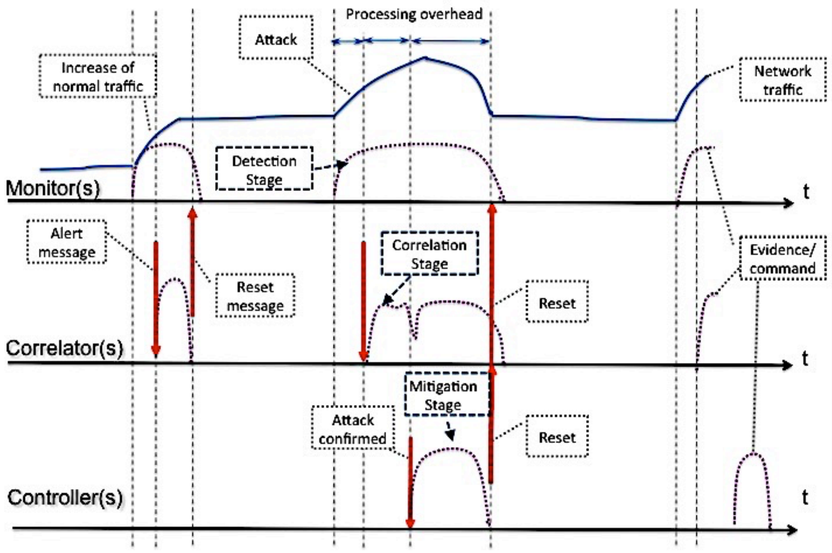
Challenges

- Intrusion Detection Systems (IDSs) cannot inspect every packet;
- Different network locations have complementary views of a DDoS attack;
- Demand of rapid detection and forensic accuracy is never ending.

Key Observations

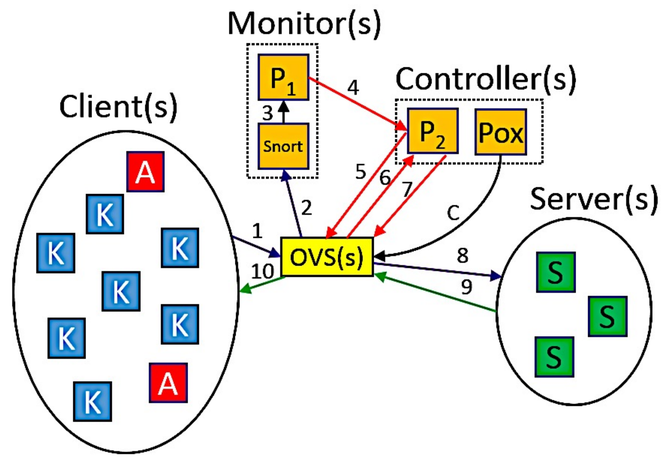
- Discrete attack signature constituents desire differential treatments;
- SDN controllers posses critical information but could be performance bottlenecks;
- IDS elements can communicate in informed and targeted packet inspection.

Collaborative Detection/Mitigation

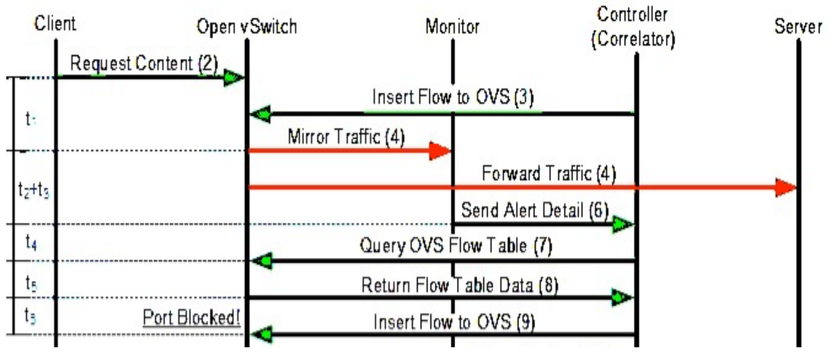


Technical Approach

- Distributed Monitors quickly raise alerts to traffic irregularities;
- SDN Controllers activate attack Correlators to inspect selected packets on demand;
- If attacked confirmed, OpenFlow APIs are used to drop/redirect attack traffic;
- This collaborative scheme is implemented on GENI.

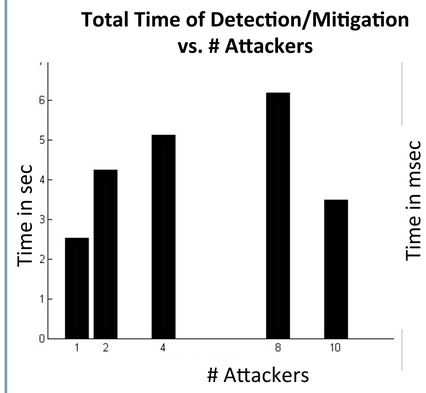


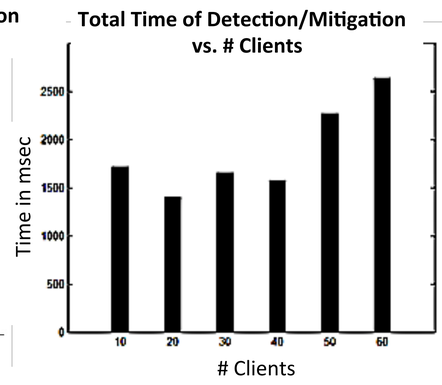
Communication

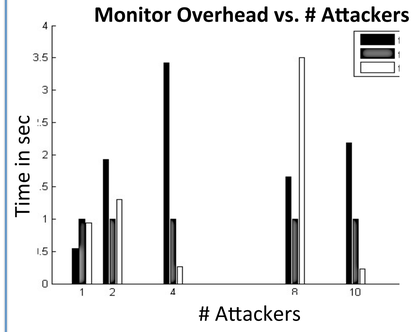


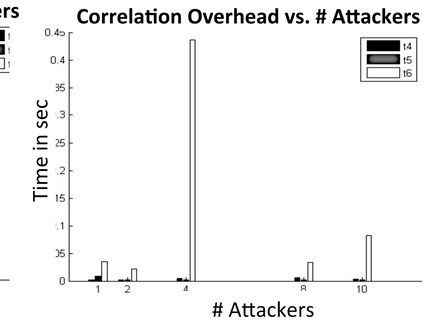
Results

- Number of regular nodes
- Number of attacker nodes
- Topology of attackers, victim, and regular users









Conclusion and Future Work

- Solutions realize the full capabilities of SDN;
- Our approach is applicable to a large-scale network for DDoS flooding detection and containment;
- Future work includes:
  - Comprehensive experimentation;
  - Extension to other security applications, e.g., APT and covert channel detection/mitigation.