DaMask: Cloud DDoS Defense Mechanism
Using Software Defined Networking

Mortada Aman

Department of Electrical & Computer Engineering
Missouri University of Science and Technology

maaf4d@mst.edu
DaMask: Cloud DDoS Defense Mechanism Using Software Defined Networking

• Introduction
• Model Design
• Evaluation
• Conclusion
DaMask: Cloud DDoS Defense Mechanism Using Software Defined Networking

- Introduction
- Model Design
- Evaluation
- Conclusion
Introduction

• Cloud Computing: provides remote data storage and computation for low cost
• Software Defined Networking (SDN): High-level network management
• The two can be combined to increase the security of Cloud Computing and defend against Distributed Denial of Service (DDoS) attacks
DaMask: Cloud DDoS Defense Mechanism

Introduction

- Existing DDoS defense mechanism assume that the networks are fully controlled by the admins
- DaMask does not make this assumption since that it is not the case in most networks
- DaMask is a DDoS attack mitigation architecture using software-defined networking
DaMask: Cloud DDoS Defense Mechanism Using Software Defined Networking

• Introduction
• Model Design
• Evaluation
• Conclusion
DaMask: Cloud DDoS Defense Mechanism

Model Design

• This paper aims to achieve the following:
  – Enhance the security and DDoS defense by combining cloud computing with SDN
  – Propose a highly scalable and flexible DDoS attack mitigation architecture: DaMask
  – Introduce a model update phase to detect new complex attacks (DaMask-D)
  – Implement the structure and evaluate it using simulation on Amazon EC2 clouds
DaMask: Cloud DDoS Defense Mechanism

Model Design

• DaMask analyzes the effectiveness of the defense mechanism on hybrid clouds

• Cloud computing properties:
  – Cloud providers control the network
  – Resource allocation and virtualization can be used to change the network topology
  – All users share the same network infrastructure

• Cloud Computing Challenges:
  – Public accessibility
  – Dynamic network allocation
DaMask: Cloud DDoS Defense Mechanism
Model Design

Fig. 1. The structure of a hybrid cloud, consisting of one private cloud and two public clouds. Five types of attack traffic are shown in the figure.
DaMask: Cloud DDoS Defense Mechanism
Model Design

- SDN separates the control plane from the data plane and allows the network control (application) to take over the control plane.

- SDN important properties:
  - Centralized network control
  - Simplified packet forward
  - Software based network function implementation
  - Virtualized networks
DaMask: Cloud DDoS Defense Mechanism
Model Design

Model design’s requirements:
- Effective: Virtualization and slicing
- Small overhead: reduce communication overhead while speeding up detection
- Inexpensive: fast re-configuration scheme to avoid disruption

DaMask consists of two modules:
- DaMask-D: Anomaly-based detection system
- DaMask-M: Attack reaction system
DaMask: Cloud DDoS Defense Mechanism

Model Design

Fig. 2. Workflow of DaMask.
DaMask: Cloud DDoS Defense Mechanism Using Software Defined Networking

- Introduction
- Model Design
- Evaluation
- Conclusion
DaMask: Cloud DDoS Defense Mechanism

Setup

Fig. 3. The simulated hybrid cloud topology.
DaMask: Cloud DDoS Defense Mechanism Using Software Defined Networking

• Overhead
  – Computation Cost: 3 aspects:
    • Offline training process
    • Online testing process
    • Model updating process: local and global
    • Local update is cheaper than global
  – Communication: only related to round trip time between clouds (constant overhead)
  – Overall relatively small

• Topology change: DaMask can adapt to topology changes caused by virtualization
DaMask: Cloud DDoS Defense Mechanism Using Software Defined Networking

Table 1
Communication time.

<table>
<thead>
<tr>
<th>Task</th>
<th>Basic</th>
<th>DaMask w/o test</th>
<th>DaMask w/ test</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>West</td>
<td>East</td>
<td>West</td>
</tr>
<tr>
<td>Ping (ms)</td>
<td>196</td>
<td>12</td>
<td>425</td>
</tr>
<tr>
<td>Http (s)</td>
<td>2.4</td>
<td>1.7</td>
<td>2.3</td>
</tr>
<tr>
<td></td>
<td>462</td>
<td>85</td>
<td>2.4</td>
</tr>
</tbody>
</table>
DaMask: Cloud DDoS Defense Mechanism Using Software Defined Networking

- Detection
  - Data shift Solution: three kinds of updates are introduced: basic, local, and global
  - Accuracy: Table 2 for basic, local, and global

<table>
<thead>
<tr>
<th>Table 2</th>
<th>Detection accuracy.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Detection rate (%)</td>
</tr>
<tr>
<td></td>
<td>( \mathcal{M}_{\text{basic}} )</td>
</tr>
<tr>
<td></td>
<td>( \mathcal{M}_{\text{local}} )</td>
</tr>
<tr>
<td></td>
<td>( \mathcal{M}_{\text{global}} )</td>
</tr>
</tbody>
</table>
DaMask: Cloud DDoS Defense Mechanism Using Software Defined Networking

• Introduction
• Model Design
• Evaluation
• Conclusion
DaMask: Cloud DDoS Defense Mechanism Using Software Defined Networking

- DaMask is a defense mechanism that utilizes SDN to protect a hybrid cloud from DDoS attacks
- It updates automatically to adapt to new attacks
- It introduces three kinds of updates depending on need
- Adapts to topology change
- Relatively low overhead
- High detection rate
DaMask: Cloud DDoS Defense Mechanism Using Software Defined Networking

- Good paper overall
- They did not explain some of the features clearly (such as basic, local, and global updates)
- In general, the scheme seems promising
References and Further Reading

End of Foils