International Journal of Advanced Research in Computer Science & Technology (IJARCST)

| ISSN: 2347-8446 | www.ijarcst.org | editor@ijarcst.org |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 3, Issue 5, September-October 2020||

DOI:10.15662/IJARCST.2020.0305002

Defensive Network Architectures Against Distributed Denial-of-Service Attacks

Devdutt Pattanaik

Nanasaheb Mahadik College of Engineering, Sangli, MH, India

ABSTRACT: Distributed Denial-of-Service (DDoS) attacks persistently threaten network availability and service reliability. Designing resilient networks capable of withstanding such attacks is critical. This paper surveys architecture-level strategies and defense mechanisms developed before 2019 to bolster network resilience against DDoS threats. We categorize approaches into proactive and reactive overlays, Software-Defined Networking (SDN) and Network Functions Virtualization (NFV)-based defenses, and overlay-based session-shielding techniques. The methodology includes systematic literature analysis, performance comparison across key metrics (latency, deployment transparency, collateral damage), and integration of case studies such as Bohatei (SDN/NFV defense) and overlay frameworks like AID, WebSOS, and MOVE. Findings indicate that proactive overlays provide low latency during normal operation, while reactive overlays maintain service continuity during attacks with minimal collateral damage. SDN/NFV solutions, exemplified by Bohatei, demonstrate elastic, scalable, and responsive defense against high-throughput attacks. In Named Data Networking, Poseidon mitigates interest flooding via architectural modifications . Limitations include complexity in deployment, reliance on ISP cooperation, vulnerabilities of fixed overlay nodes, and the need for rapid detection. The proposed workflow guides deployment: threat modeling, selecting defense architecture, deploying monitoring/mitigation (e.g., SDN controllers, overlays), testing, and iterative refinement. Advantages include scalability, flexibility, and improved availability; disadvantages include cost, complexity, and potential latency during attacks. Results emphasize that hybrid models combining overlay techniques and SDN/NFV can achieve robust resilience. We conclude that multi-layered strategies are most effective, and future research should explore machine learning–enhanced detection, blockchain-assisted distributed mitigation, and real-time adaptive defense mechanisms.

KEYWORDS: Distributed Denial-of-Service (DDoS), Network Resilience, Overlay Defense, Software-Defined Networking (SDN), Network Functions Virtualization (NFV), Proactive vs. Reactive Defense, Bohatei, Poseidon (NDN)

I. INTRODUCTION

DDoS attacks, orchestrated via distributed botnets, aim to overwhelm targets with illegitimate traffic, disrupting services. The sophistication and scale of such attacks—such as memcached amplification or IoT-based botnets—have grown, challenging traditional defense mechanisms.

Resilient network design requires proactive and reactive frameworks that ensure service availability during attacks. Overlay-based architectures—like WebSOS, AID, and MOVE—create alternate communication paths using authenticated proxies and scheduling algorithms to maintain legitimate access during attacks . Emerging paradigms like Software-Defined Networking (SDN) and Network Functions Virtualization (NFV) introduce flexibility and scalability to DDoS defense. Bohatei exemplifies this with elastic allocation of mitigation functions to counter high-rate attacks within minutes .

For new network architectures like Named Data Networking (NDN), DDoS variants like interest flooding require novel defenses; Poseidon proposes detection and mitigation mechanisms adapted to content-centric models .

Our paper systematically evaluates these strategies, comparing their effectiveness across detection latency, deployment feasibility, infrastructure transparency, and collateral damage. A structured deployment workflow, moving from threat modeling to continuous optimization, is presented. By reviewing the pre-2019 state-of-the-art, we identify key strengths and limitations, and lay groundwork for future adaptive, hybrid, and intelligent resilience frameworks.

International Journal of Advanced Research in Computer Science & Technology (IJARCST)

| ISSN: 2347-8446 | www.ijarcst.org | editor@ijarcst.org |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 3, Issue 5, September-October 2020||

DOI:10.15662/IJARCST.2020.0305002

II. LITERATURE REVIEW

Overlay-Based Defense Architectures
WebSOS, AID, and MOVE represent systems that route legitimate clients through overlay networks during DDoS attacks. These overlays engage post-attack detection (reactive), offering minimal performance impact during normal operations, negligible collateral damage, and infrastructure transparency . AID, in particular, handles insider threats via virtual packet scheduling.

SDN/NFV-Based Defenses
Bohatei demonstrates how SDN/NFV frameworks deliver elastic DDoS protection by dynamically deploying virtual mitigation functions. It handles attacks up to 500 Gbps and responds within one minute, ensuring scalability and adversary resilience .

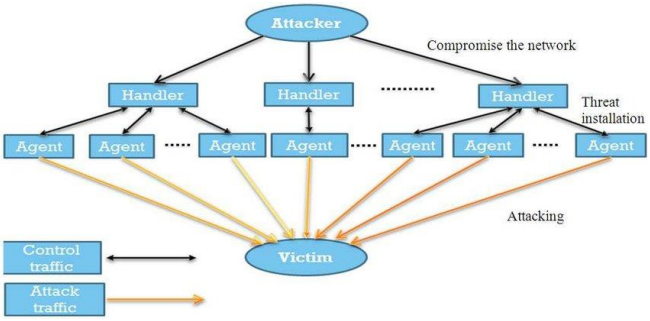
Architectural Defense in NDN
The NDN model faces unique DDoS threats like interest flooding. The Poseidon framework within NDN introduces detection and mitigation tailored to content-centric routing, marking an early defense design for future internet structures .

Classic and ISP-Level Measures
Traditional methods include IP spoofing prevention via ingress filtering (RFC 2827) and history-based filtering at network boundaries. Flooding attacks remain highly disruptive—university-level experiments show traffic drops >90% under DDoS.

This review reveals a progression: from perimeter filtering and ISP cooperation to agile overlays and programmable network resilience.

III. RESEARCH METHODOLOGY

1. **Threat Modeling**: Characterize DDoS types—volumetric, application-layer, amplification—based on historical evidence like memcached-based attacks.
2. **Defense Mechanism Survey**: Catalog proactive/reactive overlay techniques (WebSOS, AID, MOVE), SDN/NFV solutions (Bohatei), and architectural defenses (Poseidon for NDN).
3. **Evaluation Criteria**:
   - **Latency Impact**: Performance under normal vs attack conditions.
   - **Collateral Damage**: Legitimate user experience during mitigation.
   - **Deployment Complexity**: Infrastructure changes and ISP cooperation.
   - **Scalability and Elasticity**: Ability to handle increasing attack volumes or adapt in real time.
4. **Case Studies**: Analyze Bohatei's scalability and response, overlay systems' latency behavior .
5. **Synthesis of Trade-offs**: Compare techniques, outlining when overlays, SDN/NFV, or architectural protocols offer better resilience.
6. **Workflow Design**: Construct deployment framework guiding organizations through defense strategy selection, testing, and refinement.
7. **Gap Analysis**: Identify limitations and potential enhancements for future designs (e.g., adaptive routing, ML-based detection).



International Journal of Advanced Research in Computer Science & Technology (IJARCST)

| ISSN: 2347-8446 | www.ijarcst.org | editor@ijarcst.org |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 3, Issue 5, September-October 2020||

DOI:10.15662/IJARCST.2020.0305002

IV. KEY FINDINGS

1. **Overlay-Based Defense Resilience**:
   - Zero latency during normal operations, since overlays activate only upon attack detection.
   - Low collateral damage, allowing only authenticated users through (e.g., AID) .
   - Drawbacks include potential attack targeting on overlay nodes and dependency on manual detection/activation.
2. **SDN/NFV-Enabled Elastic Defense**:
   - Bohatei showcases automated, scalable defense. Capable of mitigating 500 Gbps attacks in under a minute .
   - Highly responsive and adaptable to new attack vectors.
   - Downsides: reliance on emerging infrastructure; complexity in orchestration.
3. **Content-Centric Defense (Poseidon)**:
   - Introduces DDoS mitigation by design in emerging architectures like NDN.
   - Demonstrates the importance of integrating resilience at architectural levels .
4. **Traditional Filtering Approaches**:
   - Still relevant as first-line perimeter defenses (ingress filtering, throttles), but insufficient alone for large-scale attacks .

In summary, effective resilience arises from combining overlay overlays with programmable network strategies to balance performance, flexibility, and coverage. No single approach suffices; defense-in-depth is essential.

V. WORKFLOW

1. **Assessment and Threat Profiling**:
   - Identify probable DDoS vectors (e.g., volumetric, application specific, amplification).
2. **Select Defense Strategy**:
   - **Overlay-Based** for organization without SDN/NFV infrastructure.
   - **SDN/NFV-Based** (e.g., Bohatei) if dynamic scalability is required.
   - **Architectural Solutions** (like Poseidon) for future-ready networks.
3. **Design and Provisioning**:
   - Deploy overlay proxies or virtualized mitigation nodes.
   - Configure SDN controller for flow steering and NF placement.
4. **Attack Detection and Routing Activation**:
   - Implement monitoring triggers (e.g., traffic surge detection).
   - Transition to overlay routing or instantiate virtual defense functions.
5. **Performance Monitoring**:
   - Track throughput, latency, and false positives during attack and normal operations.
6. **Post-Attack Analysis and Optimization**:
   - Adjust thresholds, scale capacity, refine detection algorithms.
7. **Iterative Refinement**:
   - Update defense configurations, expand overlay coverage, integrate new detection intelligence.

This workflow enables layered resilience strategy development suited to network capability and threat landscape.

VI. ADVANTAGES AND DISADVANTAGES

Overlay-Based Defense

- *Advantages*: Transparent in non-attack periods; minimal collateral damage; limited infrastructure changes.
- *Disadvantages*: Potential for targeted overlay attacks; activation latency; manual deployment.

SDN/NFV-Based Defense (Bohatei)

- *Advantages*: Elastic scaling; rapid response; automation.
- *Disadvantages*: High architectural complexity; dependency on NFV infrastructure.

Architectural Solutions (Poseidon/NDN)

- *Advantages*: Integrated defenses aligned to network design.
- *Disadvantages*: Requires new architecture adoption; early-stage research.

International Journal of Advanced Research in Computer Science & Technology (IJARCST)

| ISSN: 2347-8446 | www.ijarcst.org | editor@ijarcst.org |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 3, Issue 5, September-October 2020||

DOI:10.15662/IJARCST.2020.0305002

Perimeter Filtering & Conventional Methods

- *Advantages*: Simple, established.
- *Disadvantages*: Easily overwhelmed by large-scale modern attacks.

VII. RESULTS AND DISCUSSION

Overlay defense models like AID maintain service continuity with low collateral impacts during flooding attacks, but rely on timely detection and can be circumvented by targeting overlay components .

Bohatei embodies the SDN/NFV promise: defense that scales dynamically in both capacity and coverage, delivering mitigation within a minute for massive attacks .

Poseidon demonstrates resilience in NDN environments, countering interest flooding at the architectural level, illustrating the need for intrinsic security in new network models . Traditional techniques serve as necessary but insufficient layers in defense-in-depth strategies. Their combination with overlays and SDN-based routing enhances overall resilience. However, deployment complexity and cost remain practical barriers. Future enhancements should involve automated detection, ML-powered classification, and decentralized collaboration across domains.

VIII. CONCLUSION

A resilient network architecture capable of withstanding DDoS attacks requires a multi-layered defense strategy combining overlay mechanisms, SDN/NFV-based elasticity, and architecture-level protections. Overlay frameworks like AID ensure service continuity with minimal interference during normal operations. SDN/NFV platforms like Bohatei enable dynamic, scalable responses to large-scale attacks. Architectural designs like Poseidon integrate DDoS resilience into future networking paradigms. No single technique is sufficient; deployment depends on infrastructure capabilities and threat profiles. A defense-in-depth approach harnesses the strengths of each method while mitigating weaknesses. Implementing an iterative workflow—from threat modeling to real-time adaptation—is essential.

IX. FUTURE WORK

1. **Machine Learning–Driven Detection**: Incorporating behavioral analysis for real-time detection of nuanced or stealth attacks.
2. **Automation & Orchestration**: Enhancing SDN/NFV frameworks to auto-scale mitigation as a function of attack severity.
3. **Distributed Overlay Defense**: Mitigating overlay targeting via decentralized proxy networks or peer cooperation.
4. **Cross-Domain Collaboration**: Sharing threat intelligence and mitigation strategies across ISPs and cloud providers.
5. **Blockchain-Aided Trust**: Securely coordinating defense across domains using decentralized trust systems.
6. **Architectural Resilience in Future Network Protocols**: Embedding DDoS resistance in emerging paradigms (e.g., NDN, IoT-centric models).

Through these advances, future networks can be more adaptive, automated, and resilient against evolving DDoS threat landscapes.

REFERENCES

1. Kaur, R., Sangal, A. L., & Kumar, K. (2017). Overlay based defensive architecture to survive DDoS: A comparative study. *Journal of Homeland Security*, SAGE .
2. Fayaz, S. K., Tobioka, Y., Sekar, V., & Bailey, M. (2015). A New Approach to DDoS Defense using SDN and NFV (Bohatei). *preprint* .
3. Compagno, A., Conti, M., Gasti, P., & Tsudik, G. (2013). Poseidon: Mitigating Interest Flooding DDoS Attacks in Named Data Networking. *preprint* .
4. Askar, S. (2015). Investigation of the Impact of DDoS Attack on Network Efficiency... .
5. Tipton H. & Krause M. (2004); Chang R.K.C. (2002); Ioannidis & Bellovin (2002). DDoS defense strategies including Pushback, ingress filtering