

**MITIGASI SERANGAN DDOS PADA JARINGAN *SOFTWARE
DEFINED NETWORKING* (SDN) MENGGUNAKAN IDS,
FIREWALL, DAN LOAD BALANCING**

SKRIPSI

Diajukan untuk memenuhi salah satu syarat mencapai derajat Sarjana
Program Studi Teknik Komputer



Disusun oleh

OKTAVIANA NOVIA BARUNG

21.83.0635

Kepada

**FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA**

2026

MITIGASI SERANGAN DDOS PADA JARINGAN *SOFTWARE DEFINED NETWORKING* (SDN) MENGGUNAKAN IDS, FIREWALL, DAN LOAD BALANCING

SKRIPSI

untuk memenuhi salah satu syarat mencapai derajat Sarjana

Program Studi S1 Teknik Komputer



disusun oleh

OKTAVIANA NOVIA BARUNG

21.83.0635

Kepada

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

2026

HALAMAN PENGESAHAN

SKRIPSI

MITIGASI SERANGAN DDOS PADA JARINGAN *SOFTWARE DEFINED NETWORKING* (SDN) MENGGUNAKAN IDS, FIREWALL, DAN LOAD BALANCING

Yang disusun dan diajukan oleh

Oktaviana Novia Barung
21.83.0635

telah disetujui oleh Wahid Miftahul Ashari, S.Kom., M.T
pada tanggal 20 April 2026

Dosen Pembimbing,


Wahid Miftahul Ashari, S.Kom., M.T
NID. 190302452

HALAMAN PENGESAHAN

SKRIPSI

MITIGASI SERANGAN DDOS PADA *SOFTWARE DEFINED NETWORKING* (SDN) MENGGUNAKAN IDS, FIREWALL, DAN LOAD BALANCING

Yang disusun dan diajukan oleh

Oktaviana Novia Barung

21.83.0635

Telah dipertahankan di depan dewan penguji
pada tanggal 20 April 2026

Susunan Dewan Penguji

Nama penguji

Senie Destva, S.T., M.Kom.
NIK.190302312

Jeki Kuswanto, S.kom., M.Kom.
NIK. 190302456

Wahid Miftahul Ashari, S.Kom., M.T.
NIK.190302452

Tanda tangan



Skripsi ini telah diterima sebagai salah satu
persyaratan untuk memperoleh gelar Sarjana Komputer
tanggal 20 april 2025

DEKAN FAKULTAS ILMU KOMPUTER



Prof. Dr. Kursini, M.Kom.
NIK. 190302106

HALAMANA PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

Nama mahasiswa : Oktaviana Novia Barung

NIM : 21.83.0635

Menyatakan bahwa Skripsi dengan judul berikut:

Mitigasi Serangan DDoS Pada Jaringan *Software Defined Networking* (SDN) Menggunakan IDS, Firewall, dan Load Balancing.

Dosen Pembimbing : Wahid Miftahul Ashari, S.Kom., M.T.

1. Karya tulis ini adalah benar-benar ASLI dan BELUM PERNAH diajukan untuk mendapatkan gelar akademik, baik di Universitas AMIKOM Yogyakarta maupun di Perguruan Tinggi lainnya.
2. Karya tulis ini merupakan gagasan, rumusan dan penelitian SAYA sendiri, tanpa bantuan pihak lain kecuali arahan dari Dosen Pembimbing.
3. Dalam karya tulis ini tidak terdapat karya atau pendapat orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan disebutkan dalam Daftar Pustaka pada karya tulis ini.
4. Perangkat lunak yang digunakan dalam penelitian ini sepenuhnya menjadi tanggung jawab SAYA, bukan tanggung jawab Universitas AMIKOM Yogyakarta.
5. Pernyataan ini SAYA buat dengan sesungguhnya, apabila di kemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka SAYA bersedia menerima SANKSI AKADEMIK dengan pencabutan gelar yang sudah diperoleh, serta sanksi lainnya sesuai dengan norma yang berlaku di Perguruan Tinggi.

Yogyakarta, 20 April 2026

Yang Menyatakan,



Oktaviana Novia Barung

HALAMAN PERSEBAHAN

Dengan penuh rasa syukur kehadiran Tuhan yang Maha Esa atas berkat dan rahmatnya, karya sederhana ini saya persembahkan kepada orang yang telah mendukung, membimbing, dan menyemangati dalam peroses penyelesaian skripsi ini. Oleh karena itu, dengan penuh rasa hormat dan terima kasi, laporan ini penulis persembahkan kepada:

1. Papa, Mama, dan adiku, terima kasih atas doa yang tidak pernah terputus, kasih sayang yang selalu menguatkan, serta pengorbanan yang tak terhingga. Segala pencapaian ini tidak lepas dari dukungan dan kepercayaan yang diberikan kepada saya.
2. keluarga besar, terima kasih atas perhatian, dukungan, dan motivasi yang diberikan
3. Bapak Wahid Miftahul Ashari, S.Kom., M.T. selaku dosen pembimbing saya, terima kasih telah membimbing dengan sabar, memberikan arahan, serta meluangkan waktu dan perhatian selama peroses penyusunan skripsi ini.
4. Untuk teman-teman saya, terima kasih karena selalu ada dalam setiap peroses, baik saat tertawa maupun saat Lelah. Kebersamaan, dukungan, dan kepedulian yang kalian berikan membuat perjalanan ini terasa lebih ringan.
5. Dan kepada idola saya Bangtan, terima kasih atas karya dan pesan-pesan yang disampaikan untuk selalu percaya pada peroses, menerima kekurangan diri, dan tetap melangkah meskipun tidak selaluh muda.

KATA PENGANTAR

Puji dan Syukur penulis panjatkan ke hadirat Tuhan Yang Maha Esa atas segala Rahmat dan karunianya sehingga penulis dapat menyelesaikan penelitian ini dengan baik. Penelitian yang berjudul “Mitigasi Serangan DDoS Pada Jaringan Software Defined Networking (SDN)” ini disusun sebagai salah satu syarat untuk memperoleh gelar sarjana pada program studi Teknik Komputer, Fakultas Ilmu Komputer, Universitas Amikom Yogyakarta.

Dalam proses penyusunan skripsi ini, penulis menyadari bahwa tanpa bantuan, bimbingan, dan dukungan dari berbagai pihak, skripsi ini tidak akan dapat terselesaikan dengan baik. Oleh karena itu, pada kesempatan ini penulis menyampaikan terima kasih kepada:

1. Kedua orang tua tercinta atas doa, kasih sayang, pengorbanan, serta dukungan yang tiada henti.
2. Bapak Wahid Miftahul Ashari, S.Kom., M.T, selaku dosen pembimbing yang telah meluangkan waktu, memberi arahan, serta bimbingan yang diberikan dalam proses penelitian dan penyusunan skripsi ini.
3. Seluruh dosen program studi Teknik Komputer, Fakultas Ilmu Komputer, Universitas Amikom Yogyakarta, atas ilmu dan arahan yang telah diberikan selama masa perkuliahan.
4. Teman-teman seperjuangan yang memberikan dukungan, kerja sama, dan motivasi yang diberikan selama proses perkuliahan dan penyusunan skripsi ini.

Penulis menyadari bahwa skripsi ini masih jauh dari sempurna. Oleh karena itu, kritik dan saran yang membangun sangat diharapkan demi perbaikan dan penyempurnaan di masa yang akan datang. Semoga skripsi ini dapat memberikan manfaat bagi pembaca serta berkontribusi dalam pengembangan ilmu pengetahuan, khususnya di bidang keamanan keamanan siber.

Yogyakarta, 20 April 2026

Penulis

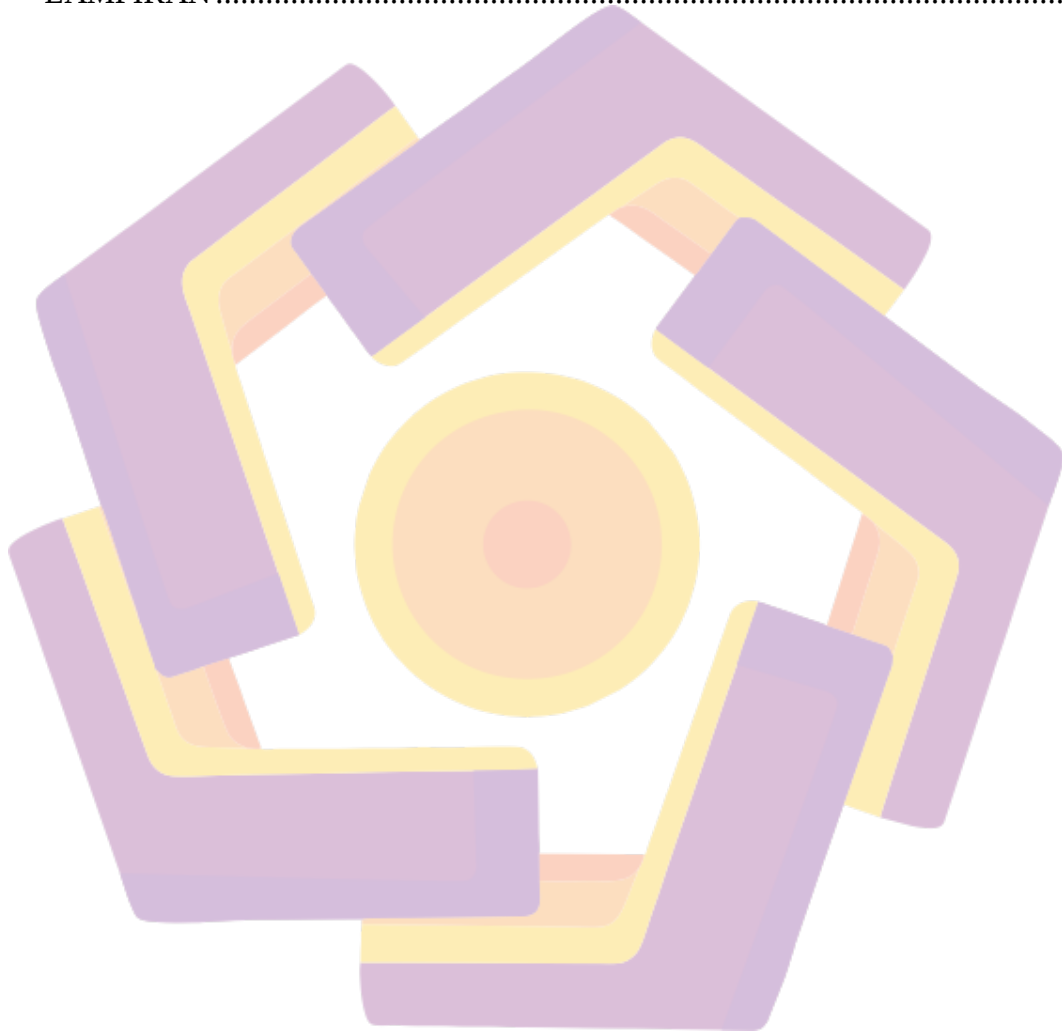
DAFTAR ISI

HALAMAN PENGESAHAN	iii
HALAMANA PERNYATAAN KEASLIAN SKRIPSI	v
HALAMAN PERSEBAHAN	vi
KATA PENGANTAR	vii
DAFTAR ISI	viii
DAFTAR TABEL	xii
DAFTAR GAMBAR.....	xiii
DAFTAR LAMBANG DAN SINGKATAN.....	xiv
DAFTAR ISTILAH.....	xv
INTISARI.....	xvi
ABSTRACT	xvii
BAB I PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah.....	3
1.3 Batasan Masalah	3
1.4 Tujuan Penelitian	3
1.5 Manfaat Penelitian	4
1.6 Sistematika Penulisan.....	4
BAB II TINJAUAN PUSTAKA	6
2.1 Studi Literatur	6
2.2 Rangkuman dan Alasan Penelitian	11
2.3 Dasar Teori	12
2.3.1 Distributed Denial of Service (DDoS)	12

2.3.2 Software Defined Networking (SDN)	12
2.3.3 Mininet.....	13
2.3.4 Ryu Controlller	14
2.3.5 Topologi single3.....	15
2.3.6 OpenFlow	15
2.3.7 Hping3	16
2.3.8 Python.....	16
2.3.9 Serangan ICMP Flood	17
2.3.10 Xtrem.....	18
2.3.11 Firewall.....	18
2.3.12 Intrusion Detection System (IDS)	19
2.3.13 Load Balancing	19
2.3.14 Quality of Service (QoS)	21
2.3.15 Wireshark.....	21
2.3.16 Virtual Box.....	22
2.3.17 Ubuntu	22
BAB III METODE PENELITIAN	23
3.1 Objek Penelitian.....	23
3.2 Alur Penelitian	23
3.3 Alat dan Bahan.....	26
3.3.1 Alat Penelitian.....	26
3.3.2 Bahan Penelitian.....	27
3.4 Lingkungan Pengujian.....	27
3.5 Topologi Jaringan	28
3.6 Instalasi dan Implementasi	28

3.6.1 Instalasi Mininet.....	28
3.6.2 Instalasi Ryu Controller.....	29
3.6.3 Implementasi Ryu Controller.....	29
3.6.4 Implementasi Topologi.....	30
3.7 Skenario YI.....	32
3.7.1 Flowchart Skenario YI	33
3.7.2 Tabel Skenario YI	34
3.8 Model Mitigasi.....	36
3.8.1 Metode Mengukur Efektivitas Mitigasi.....	37
BAB IV HASIL DAN PEMBAHASAN	39
4.1 Topologi Jaringan	39
4.1.1 Skenario Pengujian.....	40
4.1.2 Tools Pengujian dan Monitoring.....	40
4.1.3 Beban Serangan.....	41
4.2 Pengujian Performa Jaringan.....	41
4.2.1 Pengujian Sebelum Serangan.....	42
4.2.2 Pengujian Pada Saat Serangan DDoS	44
4.2.3 Pengujian Setelah Serangan/ Mitigasi Aktif	47
4.3 Evaluasi Hasil Pengujian.....	50
4.3.1 Grafik Packet Loss	50
4.3.2 Grafik Delay.....	51
4.3.3 Grafik Jitter	52
4.3.4 Grafik Throughput.....	52
4.3.5 Perbandingan Keseluruhan parameter	53
4.4 Ringkasan Hasil Pengujian.....	54

BAB V KESIMPULAN DAN SARAN	55
5.1 Kesimpulan.....	55
5.2 Saran.....	55
REFERENSI.....	57
LAMPIRAN	59



DAFTAR TABEL

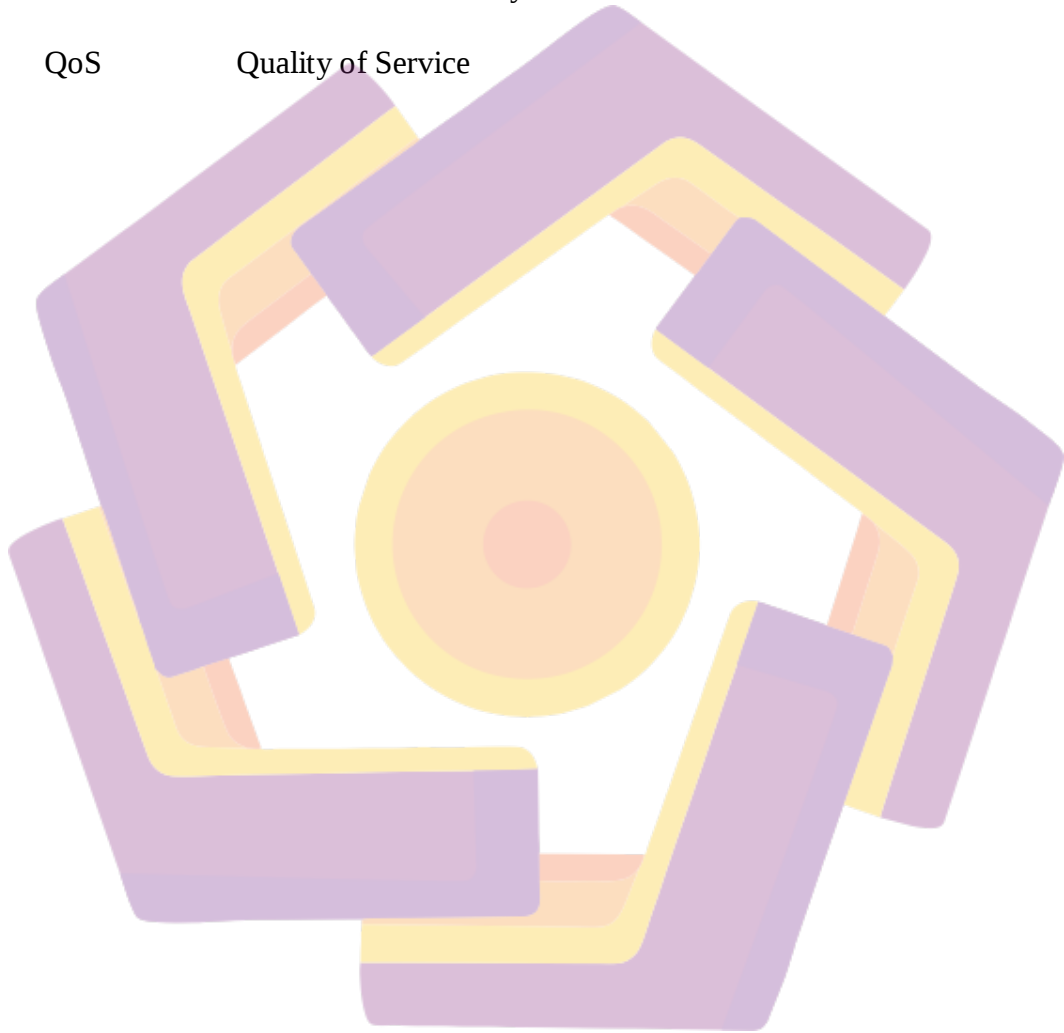
Tabel 2. 1 Keaslian Penelitian	9
Tabel 3. 1 Perangkat Keras	26
Tabel 3. 2 Perangkat Lunak	27
Tabel 3. 3 Skenario YI	34
Tabel 3. 4 Model Mitigasi	36
Tabel 3. 5 Pengukuran Eektivitas Mitigasi	38
Tabel 4. 1 IP Address	40
Tabel 4. 2 Tools Pengujian	40
Tabel 4. 3 Beban/Serangan	41
Tabel 4. 4 Hasil Uji Parameter Sebelum Serangan	44
Tabel 4. 5 Hasil Uji Parameter Saat Serangan	47
Tabel 4. 6 Hasil Uji Parameter Setelah Mitigasi Aktif	50
Tabel 4. 7 Perbandingan Keseluruhan Parameter	53

DAFTAR GAMBAR

Gambar 2. 1 Arsitektur Jaringan SDN.....	13
Gambar 2. 2 Arsitektur Ryu Controller	15
Gambar 3. 1 Alur Penelitian.....	24
Gambar 3. 2 Tampilan Ryu Controller	30
Gambar 3. 3 Running Topologi.....	31
Gambar 3. 4 Flowchart Skenario Yi.....	33
Gambar 4. 1 Topologi Single,3	39
Gambar 4. 2 Hasil Pingall Sebelum Serangan	42
Gambar 4. 3 Hasil Pengujian Delay Sebelum Serangan.....	43
Gambar 4. 4 Nilai Jitter Berdasarkan MDEV (Mean Deviation).....	43
Gambar 4. 5 Nilai Throughput Sebelum Serangan.....	44
Gambar 4. 6 h3 Menyerang Menggunakan hping3	45
Gambar 4. 7 Hasil Pingall Saat Serangan	46
Gambar 4. 8 Nilai packet loss, delay, dan jitter saat serangan.....	46
Gambar 4. 9 Nilai throughput saat serangan.....	47
Gambar 4. 10 Log hasil mitigasi	48
Gambar 4. 11 Hasil pingall setelah serangan	48
Gambar 4. 12 Nilai packet loss, delay, dan jitter setelah serangan/mitigasi aktif.....	49
Gambar 4. 13 Nilai Throughput Setelah Serangan/Mitigasi Aktif.....	50
Gambar 4. 14 Grafik Perbandingan keseluruhan Packet loss	51
Gambar 4. 15 Grafik Perbandingan Keseluruhan Delay	51
Gambar 4. 16 Grafik Perbandingan Keseluruhan Jitter.....	52
Gambar 4. 17 Perbandingan Keseluruhan Nilai Throughput.....	53

DAFTAR LAMBANG DAN SINGKATAN

DDoS	Distributed Denial of Service
SDN	Software Defined Networking
IDS	Intrusion Detection System
QoS	Quality of Service



DAFTAR ISTILAH

- SDN (Software Defined Networking)
Arsitektur jaringan yang memisahkan control plane dari data plane dalam perangkat keras, menjadikan terpusat dan dapat deprogram melalui perangkat lunak.
- DDoS (Distributed Denial of Service)
Serangan siber dengan tujuan membanjiri target dengan lalu lintas berbahaya
- IDS (Intrusion Detection System)
System keamanan yang memantau lalu lintas jaringan atau perangkat untuk mendeteksi aktivitas berbahaya, mencurigakan, atau pelanggaran kebijakan.
- QoS (Quality of Service)
Teknologi manajemen lalu lintas jaringan yang memprioritaskan data untuk menjamin kinerja yang andal

INTISARI

Serangan Distributed Denial of Service (DDoS) pada Software Defined Network (SDN) menjadi ancaman yang signifikan karena dapat mengganggu ketersediaan layanan serta menurunkan keandalan infrastruktur jaringan. Salah satu bentuk serangan yang umum terjadi adalah ICMP Flood, yaitu serangan yang membanjiri target dengan paket ICMP dalam jumlah besar sehingga sumber daya jaringan tidak mampu melayani permintaan pengguna secara normal. Pada arsitektur SDN, kondisi ini berpotensi memberikan dampak lebih besar karena controller berperan sebagai pusat pengendalian jaringan. Oleh karena itu, diperlukan mekanisme deteksi dan mitigasi yang mampu menjaga stabilitas jaringan serta meminimalkan dampak serangan terhadap kualitas layanan.

Penelitian ini mengimplementasikan mekanisme mitigasi serangan DDoS pada jaringan SDN dengan mengintegrasikan Intrusion Detection System (IDS), firewall, dan load balancing pada Ryu Controller. Simulasi dilakukan menggunakan Mininet dengan tiga skenario pengujian, yaitu kondisi normal, saat serangan ICMP Flood berlangsung, dan setelah mitigasi diaktifkan. Parameter evaluasi yang digunakan meliputi packet loss, delay, jitter, dan throughput. Hasil pengujian menunjukkan bahwa serangan menyebabkan peningkatan signifikan pada delay, jitter, throughput menurun, serta packet loss mencapai lebih dari 33.6%. Setelah mekanisme mitigasi diaktifkan, nilai delay dan jitter menurun secara signifikan, nilai throughput naik dan packet loss kembali 0%, sehingga performa jaringan kembali stabil. Dengan demikian, mekanisme mitigasi yang diterapkan terbukti efektif dalam mengurangi dampak serangan DDoS pada jaringan SDN.

Kata Kunci: DDoS, SDN, mitigasi, mininet, Icmp Flood

ABSTRACT

Distributed Denial of Service (DDoS) attacks on Software-Defined Networks (SDNs) pose a significant threat because they can disrupt service availability and reduce the reliability of network infrastructure. One common form of attack is the ICMP Flood, which floods a target with a large number of ICMP packets, rendering network resources unable to properly serve user requests. In an SDN architecture, this situation has the potential to have a greater impact because the controller acts as the central control center of the network. Therefore, detection and mitigation mechanisms are needed to maintain network stability and minimize the impact of attacks on service quality.

This study implemented a DDoS attack mitigation mechanism on an SDN network by integrating an Intrusion Detection System (IDS), firewall, and load balancing into the Ryu Controller. Simulations were conducted using Mininet with three test scenarios: normal conditions, during an ICMP Flood attack, and after mitigation was activated. Evaluation parameters used included packet loss, delay, jitter, and throughput. The test results showed that the attack caused a significant increase in delay, jitter, decreased throughput, and packet loss of over 33.6%. After the mitigation mechanism was activated, delay and jitter values decreased significantly, throughput increased, and packet loss returned to 0%, stabilizing network performance. Thus, the implemented mitigation mechanism proved effective in mitigating the impact of DDoS attacks on SDN networks.

Keyword: DDoS, SDN, mitigation, mininet, Icmp Flood