applied sciences

MDPI

Article

A Novel Approach for Efficient Mitigation against the SIP-Based DRDoS Attack

Ismail Melih Tas [1] and Selcuk Baktir [2,*]

[1] Department of Computer Engineering, Faculty of Engineering and Natural Sciences, Bahcesehir University, Istanbul 34353, Turkey
[2] College of Engineering and Technology, American University of the Middle East, Egaila 54200, Kuwait
* Correspondence: selcuk.baktir@aum.edu.kw

Abstract: Voice over Internet Protocol (VoIP) and its underlying Session Initiation Protocol (SIP) are widely deployed technologies since they provide an efficient and fast means of both voice and data communication over a single network. However, in spite of their advantages, they also have their security threats due to the inherent vulnerabilities in the underlying Internet Protocol (IP) that can potentially be exploited by hackers. This study introduces a novel defense mechanism to effectively combat advanced attacks that exploit vulnerabilities identified in some less-known features of SIP. The SIP-DRDoS (SIP-based distributed reflection denial of service) attack, which can survive the existing security systems, is an advanced attack that can be performed on an SIP network through the multiplication of legitimate traffic. In this study, we propose a novel defense mechanism that consists of statistics, inspection, and action modules to mitigate the SIP-DRDoS attack. We implement the SIP-DRDoS attack by utilizing our SIP-based audit and attack software in our VoIP/SIP security lab environment that simulates an enterprise-grade SIP network. We then utilize our SIP-based defense tool to realize our novel defense mechanism against the SIP-DRDoS attack. Our experimental results prove that our defense approach can do a deep packet analysis for SIP traffic, detect SIP flood attacks, and mitigate them by dropping attack packets. While the SIP-DRDoS attack with around 1 Gbps of traffic dramatically escalates the CPU (central processing unit) usage of the SIP server by up to 74%, our defense mechanism effectively reduces it down to 17% within 6 min after the attack is initiated. Our approach represents a significant advancement over the existing defense mechanisms and demonstrates the potential to effectively protect VoIP systems against SIP-based DRDoS attacks.

Keywords: Session Initiation Protocol; SIP; SIP security; Voice over IP; VoIP security; denial of service; DoS; distributed denial of service; DDoS; distributed reflection denial of service; DRDoS

check for updates

Citation: Tas, I.M.; Baktir, S. A Novel Approach for Efficient Mitigation against the SIP-Based DRDoS Attack. *Appl. Sci.* **2023**, *13*, 1864. https://doi.org/10.3390/app13031864

Academic Editor: Luis Javier Garcia Villalba

Received: 29 November 2022
Revised: 19 January 2023
Accepted: 26 January 2023
Published: 31 January 2023

Copyright: © 2023 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

The Voice over Internet Protocol (VoIP) and the underlying Session Initiation Protocol (SIP) are widely used for building next-generation networks and unified communication systems. They also have application areas such as network mobility management and service provisioning in mobile ad hoc networks (MANETs) [1–3]. Due to its real-time nature, SIP communication is more sensitive to quality-of-service (QoS) parameters than other signaling protocols. Considering the fact that jitter, latency, and similar problems jeopardize any telecommunication channel, the faster User Datagram Protocol (UDP) is preferred over the Transmission Control Protocol (TCP) in SIP communication for reducing server load and improving call quality. However, unlike TCP-based applications, VoIP/SIP applications inherit vulnerabilities and security risks due to the use of UDP. Data transmission in the VoIP stack is vulnerable to existing threats against IP networks which presents an intrinsic security risk to VoIP systems [4,5]. The Communication Fraud Control Association's (CFCA) Fraud Survey report gives the worldwide telecom revenue estimate as USD 2.30 trillion and loss estimate as USD 29.2 billion for 2017 [6]. Of these losses, USD 1.29 billion are

estimated to result from the exploitation of device, network, or configuration weaknesses (https://www.cfca.org/fraudlosssurvey (accessed on 25 January 2023)).

Internet telephony and video calls are the main applications of SIP [7]. SIP specifies the details of the signaling messages that govern calls between endpoints. It is used to create, modify, and terminate sessions that consist of one or more media streams [8]. In the reflection attack, the victim is tricked to respond to the challenge sent by the attacker. If multipoint communication is performed between the source and destination in a distributed denial-of-service (DDoS) attack, this is called a distributed reflection denial-of-service (DRDoS) attack [9]. In DRDoS attacks, reflectors are used between the source and the destination, which results in dramatically stronger attacks than the traditional DDoS attacks [10,11]. In this attack, the IP address of the victim is spoofed and a request for information is sent over UDP to reflectors who normally respond to this request [12,13]. Reflectors respond to the request by sending a message to the victim.

In our earlier work, we combined the vulnerabilities in the retransmission and reflection mechanisms of SIP by using the IP spoofing technique [14,15]. Our resulting attacks proved to bypass existing network protection systems such as firewalls and intrusion detection/prevention systems (IDS/IPS), in addition to black-lists and IP-address/packet-count-based rate-limiting countermeasures.

In this paper, we present a novel defense mechanism for mitigating SIP-based DRDoS attacks. Our approach is unique in that it combines both statistical and packet-level analysis to accurately identify and respond to SIP-based DRDoS attacks that are often difficult to detect due to their use of the reflection and the retransmission mechanisms. Overall, our defense mechanism provides a comprehensive approach to mitigating SIP-based DRDoS attacks and can be easily integrated into existing SIP networks.

Our Main Contributions:

- We present an improved defense approach and show its efficacy for mitigating the SIP-based DRDoS attack. The proposed enhanced defense mechanism consists of statistics, inspection, and action modules. The statistics module has SIP protocol sniffing and analysis capabilities to perform real-time monitoring of the network traffic and detect attacks. The inspection module has a deep protocol analyzer that is triggered in case of an anomaly. It creates dynamic rate-limiting rules and checks dynamic thresholds by inspecting suspected traffic in regard to SIP specifications. The action module is unique with advanced detection, notification, and action mechanisms that are adapted to the SIP protocol specifications.
- To the best of our knowledge, this is the first study to propose a defense mechanism specifically designed to mitigate SIP-based DRDoS attacks. Our approach represents a significant advancement over the existing defense mechanisms that are often limited in their ability to effectively combat these types of attacks.
- We implement our defense mechanism successfully in a VoIP/SIP test environment that simulates a real enterprise-grade SIP network. Our experimental results show that our defense mechanism is able to do a deep packet analysis for SIP traffic and detect and mitigate ongoing SIP flood attacks by dropping attack packets and letting only legitimate packets pass through. We show that the CPU usage of the SIP proxy under an SIP-DRDoS attack with around 1 Gbps traffic is effectively reduced from 74% down to 17% within 6 min after our defense mechanism is activated.
- Our results demonstrate the potential of our defense mechanism to effectively protect VoIP systems against SIP-based DRDoS attacks which are a significant security threat to these systems. Our proposed enhanced defense approach provides a strong solution for protecting against SIP-based DRDoS attacks and can be integrated into existing security systems to improve the overall resilience of SIP networks.

2. Related Work

Denial-of-service (DoS) attacks can target any network element to disrupt the networking capabilities of the network element or the functionality of the whole system. They are considered to be one of the most alarming threats to the Internet [16–19]. DoS attacks against SIP systems can be classified into five categories as malformed message, spoofed message, invalid message flooding, legitimate message flooding, and DRDoS attacks [17]. Various SIP-based DoS attacks and associated defense mechanisms are proposed in the literature [20,21].

An RTP flooding attack is a flooding attack that causes a huge amount of valid Real-time Transport Protocol (RTP) traffic filled with bytes in a random fashion [22]. The attack keeps its target clients in the dialog phase and exhausts their bandwidth, causing the SIP server to be overloaded with unwanted traffic. A detection technique for SIP-based RTP flooding attack, named packet inspection statistical technique (PIS), was proposed in [23,24]. The proposed technique comprised an initial feature extraction stage and a decision stage. The technique used the Hellinger distance parameter to compute the difference between the training and test traffic. It used the attributes INVITE, 200 OK, BYE, and ACK and aimed to augment the robustness of VoIP Networks by predicting RTP attacks. However, the technique was shown to lack efficacy in real-time applications.

A VoIP fraud detection technique was proposed in [25]. The history of user profiles was recorded in a configurable manner where an administrator chose thresholds and time frames for training and profiling. In case of suspicious activity, an alarm was generated. Alarms were eventually correlated with intrusion detection systems to avoid false positives. The proposed method was effective against session hijacking through spoofing [26]; however, it did not provide support for reflection attack protection or anomaly-based detection [27].

In a study on dark-net-inflicted attacks on the global network, the Sality SIP-scan botnet was described [28]. Although this study was not straightly focused on VoIP systems, it provided detailed information on amplification attacks [29].

A defense and monitoring model was proposed against DDoS attacks in [30]. The suggested mitigation scenarios included analyzing the network-wide DDoS security anomalies, e.g., by finding correlations with publicly available data from other networks [31]. They introduced a monitoring scheme that simulated different attacks, estimated the strength of DDoS attacks, and ultimately diminished and prevented them.

A reconfigurable real-time testbed was proposed to measure the impact of firewalls and data/voice network separation mechanisms on VoIP services [32]. The testbed enabled three levels of security, low, medium, and high, in real operating conditions. Simulations were done on a QoS basis, allowing users to test the security policies with given constraints such as network configuration, operating conditions, etc.

A technique for exploiting a VoIP softphone vulnerability was proposed in [33]. The proposed technique disabled a host by crafting SIP traffic which consumed all free memory in minutes. The authors also proposed a mitigation technique that used a context-aware filter. With the leverage of context and SIP protocol information, it became possible to deduce an SIP message that was impersonating a client. The mitigation method was fairly straightforward since softphones use predictable port numbers. Network address translation (NAT) implementation was argued to be useful for this particular purpose. Other than network-based mitigation, SIP authentication, when enforced on users, was an efficient way to mitigate such attacks.

A survey of attacks on VoIP systems, such as DoS, packet spoofing and masquerading, eavesdropping, VoIP spam and toll fraud, and related countermeasures were listed in [34]. Public Switched Telephone Network (PSTN) and VoIP networking issues were covered extensively in terms of security, and problems such as compromised signaling nodes and spoofed/fabricated signaling messages are explained.

A detection and mitigation mechanism for SIP-based DDoS attacks was described in [35,36]. The focus of these studies was on dumb message flooding attacks. Once an attack was detected, manual action needed to be taken since there was no autoresponse mechanism [37,38].

A rank correlation method (RCM) was proposed to detect DRDoS attacks in [39]. The proposed RCM used the fact that there was an inherent relationship between an attack flow and its corresponding response flow. It also used the fact that converged responsive flows had packet rates that were linearly related. According to simulation results, the RCD method distinguished reflection flows from legitimate flows successfully, and hence it could be used to detect the existence of DRDoS attacks. However, the authors did not apply or mention possible applications of their suggested method in the context of SIP networks [40].

The study in [41] focused on detecting SIP DDoS attacks and identifying attackers. An adaptive cybersecurity monitor was developed with a change-point detector to alert about an ongoing attack and identify malicious users. The main theory of detection was based on the change-point model. While they created an SIP-aware and DDoS-related solution, the study did not mention a reflection attack on the wide DDoS spectrum.

In [42], a survey of defense mechanisms against DDoS attacks was given and they were categorized as network/transport-layer-based and application-layer-based defense mechanisms. The network/transport-layer-based mechanisms were further categorized into four as network-based, source-based, destination-based, and hybrid mechanisms. Application-layer-based mechanisms were further classified as destination-based and hybrid mechanisms. SIP flooding attack mitigation was included in the category of application-layer-based mechanisms.

In [43], flooding attacks were defined as attacks that exhaust the SIP server memory by abusing the protocol's requirement to store state information. In this study, storing the states of the "To", "From" and "Call-ID" fields were repetitively exploited. Detection and mitigation algorithms were proposed against SIP flooding attacks based on an SIP white-list method. However, the proposed mechanisms did not provide a solution to SIP reflection attacks.

In [44], the authors focused on DDoS attacks against Internet-of-things (IoT) devices and highlighted the potential use of blockchain technology to address these attacks. They evaluated various existing blockchain-based solutions for mitigating DDoS attacks in the IoT environment. They surveyed and classified existing solutions into four categories as distributed-architecture-based, access-management-based, traffic-control-based, and Ethereum-platform-based. Furthermore, they analyzed these solutions in terms of their working principles, defense mechanisms, strengths, and weaknesses. While our approach is specifically focused on SIP-based DRDoS attacks and uses techniques such as statistical analysis and packet inspection, this survey paper provided an overview of blockchain-based solutions to mitigate general DDoS attacks.

In [45], a Bayesian change-point model was proposed to detect SIP flooding attacks. A real-time traffic simulator was used which was based on social network modeling. In [46], a defense mechanism was proposed for multiattribute flooding attack methods on 10 different attack occasions. In [47], deep learning techniques were used to build and train a model that learned SIP message features automatically and detected DDoS attack patterns efficiently. Our study differs from these studies as our proposed defense mechanism is based on an SIP-based DRDoS mitigation algorithm and utilizes real-time network capturing and data queuing for attack detection and mitigation.

In [48], the authors focused on detecting DDoS attacks on SIP-based VoIP networks by using a deep packet inspection (DPI)-based method. The proposed approach was based on analyzing packets to extract attack signatures and implement new detection rules. That approach was different from ours in that our approach specifically targets the SIP-based DRDoS attack. Furthermore, the response method was not mentioned for the proposed approach, and it was not mentioned whether it had the real-time capability to respond. Our approach has specialized modules for the statistical analysis and packet inspection to detect attacks, and it has the real-time capability to drop attack packets. Additionally, our approach focuses specifically on DRDoS attacks while the related work targeted general DDoS attacks.

In [49], deep forest models and service differentiation were used to filter out general DRDoS attack flows. Unlike that work, which targeted general DRDoS attacks, our

approach focuses specifically on SIP-based DRDoS attacks and utilizes a combination of statistical analysis, packet inspection, and real-time action to detect and defend against these attacks. Our proposed method is able to effectively identify DRDoS attacks with a higher detection rate and a lower false alarm rate, while also effectively eliminating attack flows and mitigating the damage caused by these attacks.

A survey of countermeasures against DoS/DDoS attacks on SIP-based VoIP networks was given with [50]. Recently introduced approaches for detecting such attacks were classified by analyzing their strengths and weaknesses. While an overview was given on various techniques for countering general DoS/DDoS attacks on SIP-based networks, the SIP-based DRDoS attack was not specifically investigated.

In our previous studies, we investigated defense mechanisms against SIP-reflection-based DDoS and DRDoS attacks and their impact on an SIP network [14,15]. In [15], we proposed an effective defense mechanism to combat SIP-reflection-based DDoS attacks. In [14], we showed how an SIP network could be attacked successfully by using the DRDoS attack. Furthermore, we suggested a defense approach to alleviate the effect of the proposed SIP-based DRDoS attack. In this current study, we further improve upon our previously suggested defense approach and provide a more detailed implementation of our defense mechanism. We demonstrate the effectiveness of our proposed defense mechanism by conducting an SIP-based DRDoS attack on an actual VoIP network and show its ability to successfully mitigate the attack.

In Table 1, we compare our study against the existing approaches in the literature, in terms of their attack types, detection methods, response methods, and real-time capabilities.

Table 1. Comparison of the related works on SIP-based DDoS defense mechanisms.

Related Work	Attack Type	Detection Method	Response Method	Real-Time Capability
[23,24]	RTP flooding	Hellinger distance	Dynamic rate limiting	Yes
[30]	DDoS	Network-wide anomaly analysis	Monitoring scheme	No
[32]	Various	Testbed simulation	Security policy and configuration	No
[33]	Softphone vuln. exploitation	Context-aware filtering	NAT implementation SIP authentication	No No
[44]	DDoS in IoT devices	Blockchain-based detection	Blockchain-based mitigation	No
[43]	Cloud-based SIP flooding	Temporal and structural fingerprints	Fingerprint whitelist DB	Yes
[46]	SIP flooding	Multidimentional sketch w/Hellinger distance	Selectively discard SIP messages	Yes
[47]	DDoS	Recurrent neural networks w/token	Discard SIP messages	Yes
[48]	SIP-based DDoS	Deep packet inspection (DPI)	New attack detection rules	Yes Yes
[49]	DRDoS	Deep forest model	Filtering w/differentiated service procedure	No
[15]	SIP-based DDoS	Statistical analysis,	Drop attack packets	Yes
Our approach	SIP-based DRDoS	Statistical analysis, packet inspection	Drop attack packets	Yes

3. Background on DoS/DDoS Attacks and Defense Mechanisms

In [14], different attack types, such as DoS/DDoS, reflection, IP-based DDoS reflection/amplification, and DDoS reflection, were evaluated in detail. An SIP server was attacked by using the IP spoofing technique and exploiting the capability to reflect SIP request/response messages. The "Via" and "Record-Route" SIP headers were targeted in the attack. It was proven that the attack could bypass existing security mechanisms. In this section, we describe possible defense mechanisms proposed in the existing works against DDoS attacks.

Snort and Zeek are two open-source network security monitoring and intrusion detection system products. Unfortunately, due to the existing security flaws in the SIP protocol specifications, these solutions have limited capabilities against SIP-based attacks. They do not have any sophisticated capability to resist SIP-DRDoS attacks.

Anomaly detection engine features are also available in several VoIP application firewalls, and VoIP IPS/IDS and SBC (session border controller) solutions. Because the SIP-DRDoS attack has the ability to overcome current security systems, new defense approaches that are specific to this type of attack need to be developed, as discussed in our previous paper [14].

Taxonomy of DDoS Defense Mechanisms

In [51], different types of DDoS defense methods proposed in the literature were analyzed in a methodical approach and a total number of twelve distinct mitigation measures against DDoS attacks were identified as follows:

- Resource accounting: privilege and behavior-based access to resources.
- Resource multiplication: increasing the bandwidth of links, deploying load balancers (a costly method).
- Resource pricing: adding a cost to resources on a computational basis.
- DoS-aware algorithms: implementing operating system (OS)-based basic algorithms that can do periodical scans.
- Traffic flow monitoring: utilizing tools to monitor network traffic to identify traffic characteristics.
- Traffic volume monitoring: sample-and-hold method and multistage filter methods.
- Source IP address monitoring: based on the fact that the source IP address is known for legitimate traffic but unknown for DDoS attack traffic.
- Monitoring other features: content and IP header filtering.
- IP hopping: detecting the change of IP address without a change in the physical location.
- Load balancing: balancing the load on servers in a multiple-server architecture for improved performance.
- TCP-migrate: migrating active TCP connections to establish a secure connection by using a cryptographic cookie and sending a new SYN request.
- Mutable service: relocation of services through a secure Domain Name System (DNS) server.

Among the above-listed general DDoS mitigation measures, we incorporated the following three in our SIP DRDoS defense mechanism: source IP address monitoring, traffic flow monitoring, and traffic volume monitoring. The main pillar of our proposed defense mechanism is traffic volume monitoring. Traffic volume monitoring is about monitoring sudden growths in the network traffic volume which is essential for mitigating DDoS attacks. We used the sample-and-hold method in our defense mechanism which is described in detail in Section 5.1.

4. Implementing the SIP-DRDoS Attack

We implemented the SIP-DRDoS attack in a VoIP/SIP test network which emulated an enterprise-grade unified communications environment with all the required software and applications. We realized the SIP registration, session initiation, and termination processes. We used Oracle Virtual Box for virtualization and installing the required operating systems [52]. We used Trixbox, an Asterisk-based IP-PBX system, as our target SIP-PBX in our

experiments [52] and dedicated a CPU core together with 512 MB memory on a MacBook PC that had a 4-core Intel Core i5 processor running 2.6 GHz and an 8 GB DDR3 memory running at 1600 MHz. By utilizing the widely used softphones Zoiper [53] and X-Lite [54] as our test clients, we simulated various types of SIP traffic and assessed the performance of the target SIP-PBX under different load conditions.

Our tool, Mr.SIP https://github.com/meliht/mr.sip (accessed on 25 January 2023), served as a multifaceted tool for simulating and analyzing SIP-based attacks. We used its SIP traffic generator, SIP client simulator, network capturing tool, and stateful SIP message flooding functionalities to perform the SIP-based DRDoS attack and to evaluate the performance of our proposed defense mechanism.

We generated random "INVITE" messages that complied with the SIP RFCs but contained no specific message patterns to bypass the detection mechanisms of anomaly detection systems. We specified target users in the "To" header of "INVITE" messages. We enumerated legitimate SIP users and wrote them to a file. We then randomly placed them in the "To" headers of generated "INVITE" messages. We syntactically generated the "User-Agent", "Via", "Contact" and "From" headers of "INVITE" messages by randomly selecting information from IP addresses and valid user agent lists. Using valid user agent lists, we randomly and syntactically generated the tag parameter in the "From" header, the values in the "Call-ID" header, and the source-port and branch parameters in the "Via" header. Using IP spoofing, we generated the source IP addresses in the "Via" and "Contact" headers. We give a pictorial description of the attack flow in Figure 1 and a sample of the INVITE messages used in the attack in Figure 2.

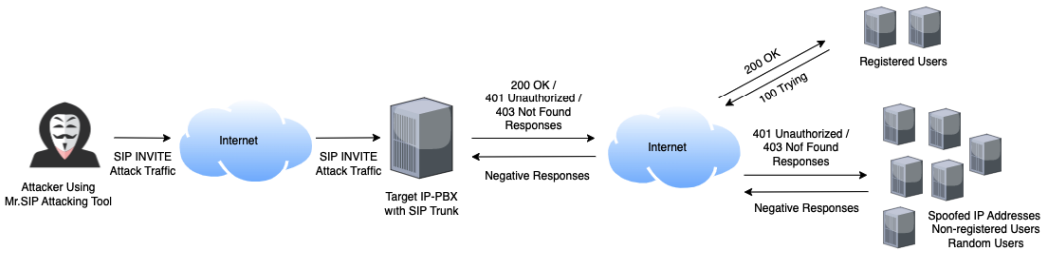


Figure 1. SIP-DRDoS attack network diagram.

```
INVITE sip:targetuser@sip-pbx.com SIP/2.0
Via: SIP/2.0/UDP 192.0.2.1:5060;branch=z9hG4bK7d87543
From: <sip:spoofeduser@192.0.2.1>;tag=9384750
To: <sip:targetuser@sip-pbx.com>
Call-ID: 84957304857@192.0.2.1
CSeq: 1 INVITE
Contact: <sip:spoofeduser@192.0.2.1:5060>
User-Agent: X-Lite release 5.0.0 stamp 73847
Content-Type: application/sdp
Content-Length: 147

v=0
o=spoofeduser 73837482748 IN IP4 192.0.2.1
s=SIP Call
c=IN IP4 192.0.2.1
t=0 0
m=audio 49170 RTP/AVP 0
a=rtpmap:0 PCMU/8000
```

Figure 2. SIP DRDoS INVITE message sample.

Since UDP is the most widely used transport protocol in SIP systems, we sent our attack messages using UDP. Network scanning and SIP enumeration need to be performed in the initial phases of a DRDoS attack against an SIP system [55]. In our DRDoS attack simulator Mr.SIP, the main components are a network scanner, SIP enumerator and DRDoS attack simulator. Utilizing random SIP message generation, SIP request reflection, and IP spoofing, our simulator successfully bypassed the embedded IDS/IPS mechanisms.

We obtained SIP client/server IP addresses and SIP user-IDs by using the network scanner and the SIP enumerator modules of our attack tool Mr.SIP. We gave as input to the network scanner the target IP address range, and the SIP component list was generated as the output. We sent an SIP OPTIONS message to all IP addresses in the provided IP address range over the UDP port 5060. By looking at the response message coming from an IP address, we were able to find out the existence of an SIP component at that address. The device was a potential SIP component if the response message was "200 OK". Similar techniques for exploring SIP networks have been previously investigated in [56,57].

As input to the SIP enumerator module, we provided the output of the network scanner module and obtained the SIP users list. We obtained SIP user information for SIP components by using the SIP enumerator module and sending SIP REGISTER messages to the SIP components in the SIP user list. If a "401 Unauthorized" message was returned, we knew that the specified user existed. On the other hand, the specified user did not exist if a "404 Not Found" message was returned.

Our SIP DRDoS attack simulator takes as input the output of the SIP enumerator module, namely, the following lists: "SIP users", "Pre-defined from users" and "Pre-defined user agents". The SIP DRDoS attack simulator has two components: an IP spoofing engine and an SIP message generator. We use the IP spoofing engine to help bypass rate-limiting defense mechanisms that exist in firewalls and intrusion detection/prevention systems [58]. IP spoofing is possible in SIP systems due to the connection-less nature of the underlying transport protocol UDP. By using spoofed IP addresses, packets coming from a single source are made to appear to originate from different IP addresses [59]. With our attack simulator, we used IP spoofing in three alternative ways: we generated counterfeit IP addresses manually, randomly, or randomly based on the subnet.

Our SIP DRDoS attack simulator module generates SIP messages that are in compliance with the SIP RFCs and acceptable by SIP components [60]. It produces random SIP INVITE and SIP REGISTER messages to avoid detection by anomaly detection systems. It puts target user information in the "To" header of generated SIP INVITE messages. A single user can be attacked, or all legitimate users can be attacked to influence the whole SIP network. The "Via", "User-agent", "From", and "Contact" headers of an SIP INVITE message are taken from enumerated lists. The "From Tag", "Branch", and "source-port" fields in the "Via" and "Call-ID" parameters/headers of the SIP INVITE message are entered as random but standards-compliant values. The IP spoofing engine component of the DRDoS attack simulator module was used to generate IP addresses for the "Contact" and "Via" headers. The architecture of our attack tool, Mr.SIP, is illustrated in Figure 3. It shows the various modules of the tool and how they interact to perform the SIP-DRDoS attack.

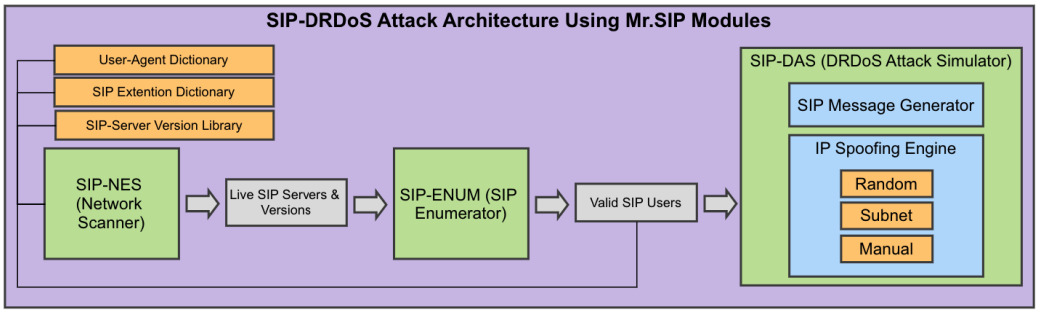


Figure 3. Architecture of Mr.SIP, the attack tool utilized in this study.

We performed the SIP-DRDoS attack by performing IP spoofing from a nonregistered user to a nonregistered user. We observed that each INVITE message was transmitted by reflectors to the target machine. Since we had nonregistered users, we observed 7 negative responses for each INVITE message [61]. The number of packets was seen to increase linearly with the number of reflectors. We measured the CPU usage of the SIP server for registered, nonregistered, and random users during the 3 min after the attack had been initiated. While a popular IP spoofing prevention technique, known as hop-count filtering [62], was active during the attack, the CPU load of the SIP server went up to 74%, 67%, and 72%, for random (registered/nonregistered), nonregistered, and registered users, respectively, as shown in Figure 4 [14].

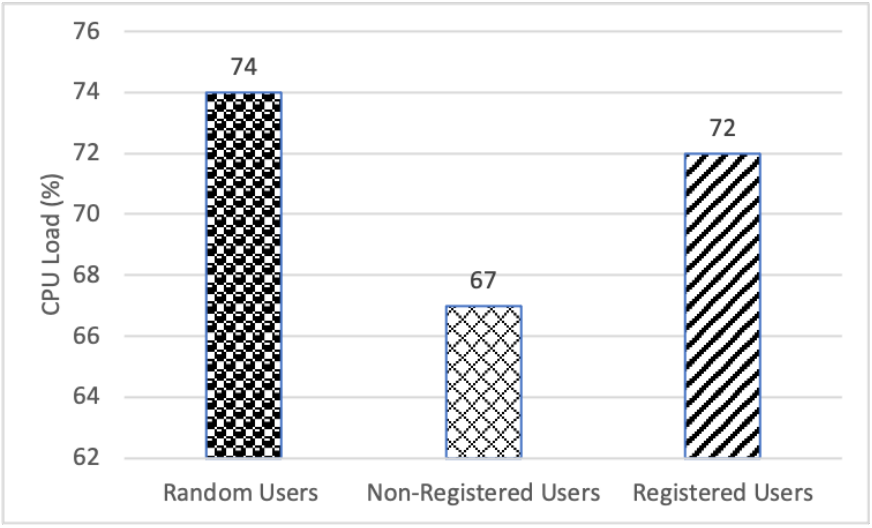


Figure 4. Average SIP server CPU loads for registered, nonregistered, and random users (3 min after the SIP-DRDoS attack was initiated).

5. A Novel Protection Mechanism against the SIP-DRDoS Attack

In this section, we present an effective mitigation mechanism against the SIP-DRDoS attack presented in Section 4. Our mechanism borrows ideas from several approaches used against existing attack scenarios [14,15]. It has SIP protocol sniffing and analysis capabilities that enable real-time network traffic monitoring. It listens to the network and performs protocol analyses to detect attacks. It utilizes multiple firewalls and IDS/IPS strategies as its working principle, giving it a powerful mechanism for attack detection and response. It possesses specially designed detection, notification, and response capabilities that are tailored to the SIP protocol specifications. At the seventh layer (application layer) of the OSI reference model, it examines each packet in the passing traffic and creates a packet and status table for each SIP communication channel in accordance with SIP specifications. These characteristics allow the proposed mechanism to execute stateful packet inspection (SPI) in the SIP protocol using application firewall features.

The proposed mechanism uses the behavior-based detection approach, as it monitors and processes differences in network traffic behavior, such as traffic rate, number of incoming requests, and number of returned responses. Using its learning mechanism, it establishes a baseline for the system and learns the typical traffic rate. It looks for deviations from the baseline, and when it finds them, it reports an alarm and, if necessary, starts an action. It does not rely on signatures to function but instead employs a customized detection algorithm to look for particular parameters and behavior when analyzing traffic. This gives it qualities that are common with heuristic detection approaches. Activity logs produce alarms when there is questionable network activity, which is then used to carry out a preset action. For instance, it can block the IP, block the port or reset the SIP session. It can also record SIP data for forensic analysis.

5.1. Proposed Defense Mechanism in Detail: Components and Workflow

Our proposed SIP DRDoS defense mechanism contains three modules: statistics module, inspection module, and action module. Each module has its own submodules as given in Figure 5 and described as follows.

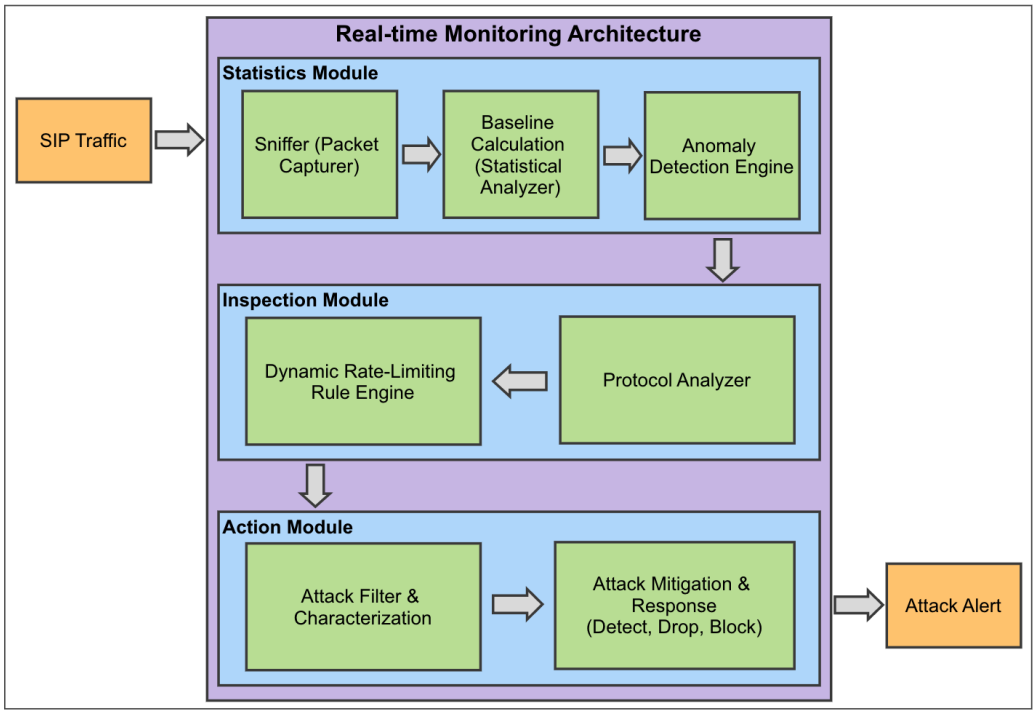


Figure 5. Proposed defense mechanism application workflow.

Statistics Module:

As given in Figure 5, the statistics module consists of three submodules: sniffer, baseline calculation, and anomaly detection engine.

The sniffer submodule filters SIP traffic by sniffing the network in real time. It captures SIP traffic periodically (hourly, daily, weekly, or monthly) and creates a reference traffic pattern, named the normal traffic pattern, taking into account the network and the SIP specifications. In order to achieve this, by taking into account the amount of traffic intensity, the system operator first determines the period of traffic sampling in terms of the number of hours, days, weeks, or months.

The baseline calculation submodule analyzes the collected sample traffic and utilizes certain threshold calculation algorithms by taking into account the SIP specifications and the baseline traffic for the duration of the sampling period. It dynamically measures the bandwidth usage and the number of packets per second to determine the lowest, highest, and average attack threshold values. The initial inbound and outbound traffic values are defined in kilobits per second. The baseline calculation submodule uses the maximum UDP SIP packet size of 64 KB globally and calculates the inbound packet rate by dividing the inbound traffic rate by the maximum UDP SIP packet size. After each sampling period, the following calculations are done by our baseline calculation mechanism, where the edge values are calculated within the pcap sample as given below:

- $Normal\ Edge$ = average network traffic rate for the sampling period;
- $Present\ Edge$ = network traffic rate at present;
- $Attack\ Edge$ = the highest momentary network traffic rate within the selected time period;
- $Suspect\ Edge = \frac{Attack\ Edge + Normal\ Edge}{2}$.

Furthermore, limit values are calculated within the pcap sample as follows:

- $Present\ Limit = \frac{Present\ Edge}{Max\ UDP\ SIP\ Packet\ Size}$;
- $Normal\ Limit = \frac{Normal\ Edge}{Max\ UDP\ SIP\ Packet\ Size}$;
- $Attack\ Limit = \frac{Attack\ Edge}{Max\ UDP\ SIP\ Packet\ Size}$;
- $Suspect\ Limit = \frac{Suspect\ Edge}{Max\ UDP\ SIP\ Packet\ Size}$.

The anomaly detection engine submodule detects anomaly states by measuring deviations from the baseline by calculating the inbound packet rate limit. When an anomaly is detected, it writes to the log, initializes an alert for the admin, and for further investigation, transmits the data to the inspection module which has a deeper protocol analyzer. Anomaly detection is achieved by using either traffic rate control or packet rate control, described as follows:

- ***Traffic rate control***: *Present Edge* and *Suspect Edge* values are compared. If *Present Edge* is larger than *Suspect Edge*, an attack is presumed, and the inspection module is triggered.
- ***Packet rate control***: If *Present Limit* is larger than *Suspect Limit*, based on the number of SIP connections per second or the number of requested packets per second, an attack is presumed and the inspection module is triggered.

Inspection Module:

As given in Figure 5, the inspection module consists of two sub-modules: a protocol analyzer and a dynamic rate-limiting rule engine.

The protocol analyzer submodule analyzes in detail the data traffic received from the anomaly detection engine according to the SIP specifications. It utilizes approaches akin to those utilized by intrusion detection systems and DDoS attack defense systems. When the rate of traffic hits the threshold value defined for attack traffic, i.e., when an anomaly is presumed, the inspection module is triggered and compares the normal and the presumed attack traffic patterns. The system keeps track of the number of call initiation packets, established sessions, reflected requests, and responses within the specified time period. It inspects the headers/tags in SIP messages, e.g., Call-ID, "from" tag, branch tag, "Via" header, and "Record-Route" header, and tries to pin down suspicious traffic so that the action module can be triggered to drop/block it.

The dynamic rate-limiting rule engine submodule creates dynamic rate-limiting rules that may trigger the action module by checking the following conditions:

- **Condition 1**: SIP connection requests coming from a single IP address are counted per second. All SIP INVITE and SIP REGISTER messages are considered incoming connections. The statistics module's rate limits are utilized to decide if the action module needs to be triggered.
- **Condition 2**: SIP connection requests directed towards a single IP address are counted per second. All SIP INVITE and SIP REGISTER messages are considered incoming connections. The statistics module's rate limits are utilized to decide if the action module needs to be triggered.
- **Condition 3**: SIP connection requests from a single IP address are counted per second, including reflected requests. The statistics module's rate limits are utilized to decide if the action module needs to be triggered.
- **Condition 4**: SIP connection requests towards a single IP address are counted per second, including reflected requests. The statistics module's rate limits are utilized to decide if the action module needs to be triggered.

Action Module:

The action module's actions comprise one passive and two active responses. When an attack is presumed, the action module puts the SIP server in one of the following modes: detect mode, drop mode, and block mode. It can also be set up to perform IP verification, before it drops/blocks packets, by rejecting incoming UDP packets and requesting them again. Each action in this module is logged and sent to the admin as an alert, as given in Figure 5. Responses by the action module are given as follows:

- ***Detect mode***: If the present rate of SIP traffic is larger than *Suspect Limit*, the system notifies the operator of a threshold violation.
- ***Drop mode***: If the present rate of the SIP traffic is larger than *Attack Limit*, SIP packets are dropped for 5 min.
- ***Block mode***: After Drop Mode is activated, if the present rate of SIP traffic is above 95% of the inbound packet rate limit, then SIP packets are blocked for 5 min.

5.2. Placement on the Network

A VoIP/SIP-based DDoS protection mechanism can be placed in multiple different locations on the network to protect the network most effectively. It can be in front of or behind the firewall. If it is placed behind the firewall, after the traffic passes through the firewall, the system starts analyzing the traffic. Thus, there is a reduction in the number of things it needs to analyze and it performs better. However, in this case, it will not be possible to know if an attack is targeting the firewall. If it is placed in front of the firewall, it will take much more traffic to analyze. However, it will have a better indicator of attacks against the firewall. In order to take advantage of both, one can place the DDoS mitigation system both in front of and behind the firewall. In this way, attacks targeting the firewall can also be examined beforehand, and not allowed to go inside. After passing through the firewall, a secondary protection system can also be positioned to examine the traffic deeper in order to search for variations in policies or for abnormalities depending on the type of system. We positioned our DRDoS mitigation system behind the firewall during our tests in this study. As shown in Figure 6, during the conduct of this study, we positioned our proposed defense mechanism against DRDoS attacks behind the firewall in our network architecture.

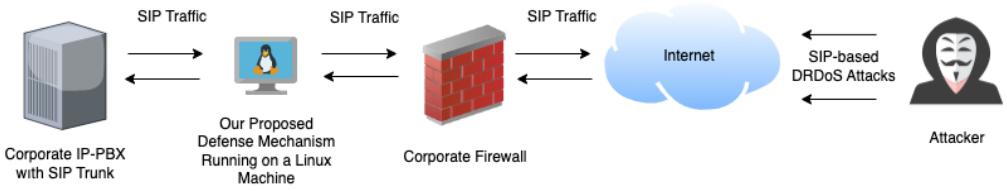


Figure 6. Placement of our proposed defense mechanism on the network.

6. Implementation Results

Our defensive tool is a DDoS defense solution that was designed exclusively for application-level SIP-based DDoS mitigation. It captures network traffic using the pcap library. As a result, asynchronous data are queued at the kernel level and subsequently analyzed for attack detection. The values for the parameters that are utilized in the calculations are in kilobits per second (kbps). It takes about 4 to 5 s to complete the calculations for the analyses. Our tool can be configured to create pcap files every hour, every day, every week or every month. It also allows us to append to pcap files. For instance, if the application is closed and reopened, it resumes sniffing the network and writing to the end of the existing pcap file from the last session. We utilized SIP-DD, our SIP-based DDoS defense tool, to implement our proposed defense mechanism against the SIP-DRDoS attack. In order to provide a better understanding of the working logic of SIP-DD, we included its pseudocode representation in Figure 7. Additionally, we made the source code for SIP-DD available on GitHub for further reference https://github.com/meliht/sip-dd (accessed on 25 January 2023).

For validating the performance of the proposed SIP-based DRDoS attack detection and mitigation mechanism, we conducted several experiments in a laboratory environment that simulated a real enterprise-grade SIP network. In these experiments, we evaluated the following performance metrics:

- ***Detection time***: the time required for the detection module to identify the presence of an attack and trigger the mitigation process;
- ***Attack intensity***: the rate at which the attack traffic is generated, measured in packets per second;

- ***CPU usage***: the percentage value of the SIP server's CPU utilization during the attack and the mitigation processes;
- ***False positive rate***: the number of legitimate traffic packets that are mistakenly identified as attack traffic and dropped by the mitigation module.

```
def defense_mechanism_workflow():
    # Capture network traffic using pcap library
    traffic = capture_network_traffic()

    # Analyze traffic for attack detection
    attack_detected = analyze_traffic(traffic)

    if attack_detected:
        # Queue data at kernel level
        data = queue_data()

        # Calculate parameters (in kbps)
        rate = calculate_rate(data)

        # Determine action based on current rate
        action = determine_action(rate)

        if action == "Detect Mode":
            # Notify operator of threshold violation if current rate is abcve Suspect Limit
            notify_operator()
        elif action == "Drop Mode":
            # Drop SIP packets for 5 minutes if current rate is above Attack Limit
            drop_packets()
        elif action == "Block Mode":
            # Block SIP packets for 5 minutes if current rate is above 95% of inbound packet rate limit
            block_packets()

        # Log action and send to administrator as alert
        log_action()

    # Configure system to create pcap files at intervals
    configure_pcap()
```

Figure 7. Pseudocode for the proposed defense mechanism using SIP-DD.

We implemented our SIP-DRDoS defense mechanism in our lab environment which simulated a real enterprise-grade SIP network. In the testing environment, where our defense mechanism resided, we first performed the SIP-DRDoS attack given in Section 4 using registered, nonregistered, and random (registered/nonregistered) users. We sent 10 K INVITE packets to the target for 6 min continuously and took performance measurements for the 6 min period from the start of the attack. Resulting from our attack, we observed a traffic intensity of over approximately 1 Gbps at the target. The performance measurements in the first 6 min of the attack (before and after the defense mechanism is activated) are given in Table 2.

Table 2. Performance measurements during the attack and defense periods.

User Type	Attack Intensity (pps)	CPU Usage during Attack (%)	CPU Usage	Detection Time (s)	False Positive Rate (%)
Random	1,000,000	74	20	12.2	0.3
Nonregistered	1,000,000	67	17	13.3	0.2
Registered	1,000,000	72	19	14.6	0.1

The defense mechanism was initiated as soon as the attack traffic reached the *attack edge* while the statistics module of our defense system was engaged. When the attack was carried out with random, nonregistered, and registered users, the detection time was found to be 12.2 s, 13.3 s, and 14.6 s, respectively. The inspection module began its investigation by triggering the specially designed dynamic rules to detect the SIP-DRDoS attack. Finally, the action module reduced the load on the target system by dropping attack packets to ensure stability.

When the SIP-DRDoS attack was applied, the SIP server's CPU usage increased to 72%, 67%, and 74% for registered, nonregistered, and random users, respectively. In Figure 8, the CPU load of the SIP server under attack is given for the first 6 min after the initiation of the attack while our defense mechanism was running. Our implementation results show that the proposed mechanism effectively performed a deep packet analysis for SIP traffic, detected the SIP-DRDoS attack, and mitigated it by dropping attack packets while letting legitimate packets pass through. While the SIP-DRDoS attack sharply increased the CPU usage of the SIP server, our defense mechanism was triggered within 3 min and mitigated the attack by dramatically reducing the CPU load in the following 3 min. As given in Figure 9, with our defense mechanism, the CPU usage of the SIP server under attack decreased from 72% down to 19%, from 67% down to 17%, and from 74% down to 20% for registered, nonregistered, and random users, respectively. Considering all types of users, the CPU usage fell from 71% down to 18% on average, as shown in Figure 10. Moreover, as given in Table 2, the false positive rate of our SIP-DRDoS attack detection mechanism was low, with only a small number of legitimate packets being mistakenly dropped. Hence, the proposed SIP-based DRDoS attack detection and mitigation mechanism exhibited good performance in terms of both detecting and mitigating the attack in real time while also maintaining a low false positive rate. These results suggested that the proposed mechanism was an effective solution for protecting SIP networks against DRDoS attacks.

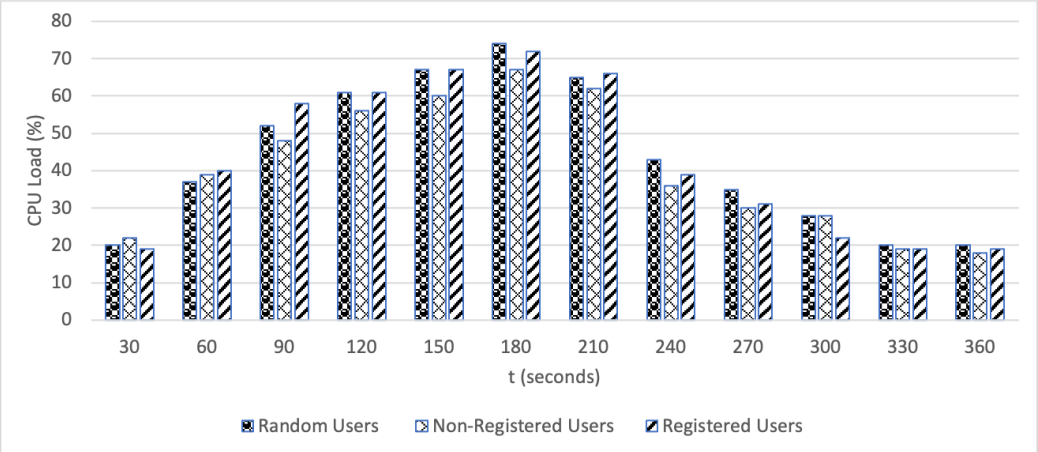


Figure 8. SIP server CPU usage for registered, nonregistered, and random users after the SIP-DRDoS attack while our defense mechanism was active.

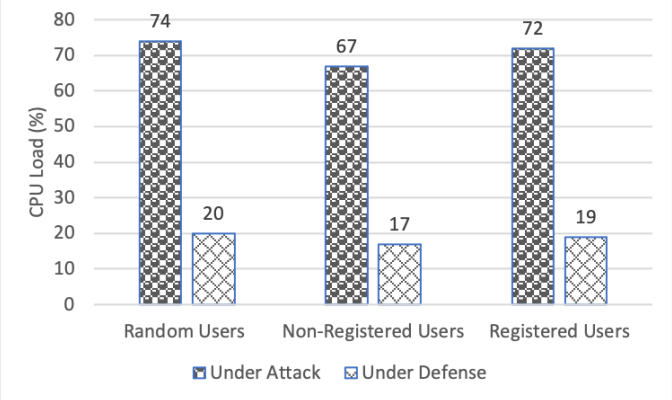


Figure 9. Average SIP server CPU loads for registered, nonregistered, and random users after the SIP-DRDoS attack and after the mitigation.

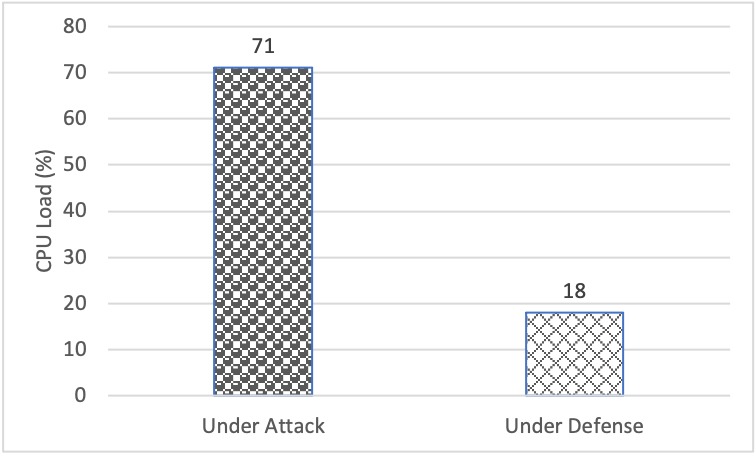


Figure 10. Average SIP server CPU load after the attack and after the mitigation for all types of users.

7. Conclusions

We implemented the SIP-DRDoS attack, which exploits vulnerabilities in UDP-based SIP signaling, in a laboratory environment that simulated a real enterprise-grade SIP network. We showed that the attack bypassed the existing defense mechanisms in an SIP network such as firewall, IDS, IPS, black-list, and IP-address/packet-count-based rate-limiting. Furthermore, we introduced and implemented an effective mitigation mechanism against the SIP-DRDoS attack. When we applied the SIP-DRDoS attack and created around 1 Gbps of traffic on the target end by sending 10K INVITE requests continuously on the originating side, the CPU load of the SIP server increased significantly up to 74% in only 3 min. However, our novel mitigation mechanism effectively pulled the CPU load down to 17% within 6 min after the initiation of the attack.

The results of our experiments demonstrate the effectiveness of the proposed approach in detecting and mitigating SIP-DRDoS attacks in real time. Our approach is based on a deep packet analysis and dynamic rate-limiting, and it is able to accurately detect and respond to SIP-DRDoS attacks while allowing legitimate traffic to pass through. Overall, our approach shows that it is possible to develop and implement effective strategies for protecting SIP systems against DRDoS attacks.

8. Discussion

One of the modern approaches to combating cyberattacks is the use of artificial intelligence (AI) to forecast and detect deviations from normal behavior [47,63–65]. While our proposed mitigation mechanism for SIP-DRDoS attacks does not specifically utilize AI, it is possible to incorporate AI techniques to further enhance its performance. For example, machine learning algorithms could be trained on historical data to recognize patterns of attack traffic and improve the accuracy of detection. As a future research direction, we identify the use of AI to optimize the attack response strategy in our mechanism, e.g., AI can be used to dynamically adjust the threshold values and determine the most effective response based on the historical training data and the context of the attack.

We would also like to note that it is important to consider the limitations and potential challenges of using AI in the context of cybersecurity. One issue is the need for a sufficiently large quantity of high-quality training data to accurately model the behavior of both normal and attack traffic. Another challenge is the possibility of adversarial attacks, where attackers attempt to manipulate or deceive the AI system. Hence, it is important to carefully design and test the robustness of any AI-based approach to ensure its effectiveness in real-world scenarios. While AI has the potential to significantly enhance the capabilities of cyberdefense systems, it is not a silver bullet and should be carefully considered in the context of the specific threat landscape and system requirements [63,65,66].

Author Contributions: Conceptualization, I.M.T. and S.B.; methodology, I.M.T.; validation, I.M.T. and S.B.; investigation, I.M.T.; writing—original draft, I.M.T.; writing—review and editing, I.M.T. and S.B.; visualization, I.M.T.; supervision, S.B. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Leu, F. A novel network mobility handoff scheme using SIP and SCTP for multimedia applications. *J. Netw. Comput. Appl.* **2009**, *32*, 1073–1091. [CrossRef]
2. Yee, Y.C.; Choong, K.N.; Low, A.L.Y.; Tan, S.W. SIP-based proactive and adaptive mobility management framework for heterogeneous networks. *J. Netw. Comput. Appl.* **2008**, *31*, 771–792. [CrossRef]
3. Bah, S.; Glitho, R.; Dssouli, R. A SIP servlets-based framework for service provisioning in stand-alone MANETs. *J. Netw. Comput. Appl.* **2013**, *36*, 147–155. [CrossRef]
4. Revathi, P. Flow and rank correlation based detection against Distributed Reflection Denial of Service attack. In Proceedings of the 2014 International Conference on Recent Trends in Information Technology, Chennai, India, 10–12 April 2014; Volume 6, pp. 10–12.
5. Tas, I.M.; Ugurdogan, B.; Tas, H. Integrating VoIP/UC Security into the Holistic Information Security Planning. In Proceedings of the 2015 23rd Signal Processing and Communications Applications Conference (SIU), Malatya, Turkey, 16–19 May 2015; Volume 23, pp. 771–792.
6. CFCA Fraud Loss Survey. 2019. Available online: https://www.cfca.org/fraudlosssurvey (accessed on 25 January 2023).
7. Bessis, T.; Gurbani, V.K.; Rana, A. Session initiation protocol firewall for the IP multimedia subsystem core. *Bell Labs Tech. J.* **2011**, *15*, 1–7. [CrossRef]
8. Johnston, A.B. *SIP: Understanding the Session Initiation Protocol*, 2nd ed.; Artech House: Boston, MA, USA, 2004; Volume 1, pp. 168–687.
9. Tsunoda, H.; Ohta, K.; Yamamoto, A.; Ansari, N.; Waizumi, Y.; Nemoto, Y. Detecting DRDoS attacks by a simple response packet confirmation mechanism. *Comput. Commun.* **2008**, *31*, 3299–3306. [CrossRef]
10. Mohana Priya, P.; Akilandeswari, V.; Mercy Shalinie, S.; Lavanya, V.; Shanmuga Priya, M. The Protocol Independent Detection and Classification (PIDC) system for DRDoS attack. In Proceedings of the 2014 International Conference on Recent Trends in Information Technology, Chennai, India, 10–12 April 2014; pp. 1–7.
11. Thomas, D.R.; Clayton, R.; Beresford, A.R. 1000 days of UDP amplification DDoS attacks. In Proceedings of the 2017 APWG Symposium on Electronic Crime Research (eCrime), Phoenix, AZ, USA, 25–27 April 2017; pp. 79–84.
12. Stanek, J.; Kencl, L. SIPp-DD: SIP DDoS Flood-Attack Simulation Tool. In Proceedings of the 20th International Conference on Computer Communications and Networks (ICCCN), Maui, HI, USA, 31 July–4 August 2011; pp. 1–7.
13. Tas, I.M.; Unsalver, B.G.; Baktir, S. Our Proposed SIP-Based Distributed Reflection Denial of Service (DRDoS) Attacks & Effective Defense Mechanism. In Proceedings of the 2nd Interdisciplinary Cyber Research Workshop 2016, Tallinn, Estonia, 2 July 2016; pp. 15–16.
14. Tas, I.M.; Unsalver, B.G.; Baktir, S. A Novel SIP Based Distributed Reflection Denial-of-Service Attack and an Effective Defense Mechanism. *IEEE Access* **2020**, *8*, 112574–112584. [CrossRef]
15. Tas, I.M.; Ugurdogan, B.; Baktir, S. Novel session initiation protocol-based distributed denial-of-service attacks and effective defense strategies. *Comput. Secur.* **2016**, *63*, 29–44. [CrossRef]
16. Bou-Harb, E.; Debbabi, M.; Assi, C. Cyber Scanning: A Comprehensive Survey. *IEEE Commun. Surv. Tutor.* **2014**, *16*, 1496–1519. [CrossRef]
17. Voznak, M.; Safarik, J. DoS Attacks Targeting SIP Server and Improvements of Robustness. *Int. J. Math. Comput. Simul.* **2012**, *6*, 177–184.
18. Paxson, V. An analysis of using reflectors for distributed denial-of-service attacks. *ACM SIGCOMM Comput. Commun. Rev.* **2001**, *31*, 38–47. [CrossRef]
19. Santanna, J.J.; van Rijswijk-Deij, R.; Hofstede, R.; Sperotto, A.; Wierbosch, M.; Granville, L.Z.; Pras, A. Booters An analysis of DDoS-as-a-service attacks. In Proceedings of the 2015 IFIP/IEEE International Symposium on Integrated Network Management (IM), Ottawa, ON, Canada, 11–15 May 2015; pp. 243–251.
20. Mirkovic, J.; Prier, G.; Reiher, P. Attacking DDoS at the source. In Proceedings of the 10th IEEE International Conference on Network Protocols, Paris, France, 12–15 November 2002; pp. 312–321.
21. Sisalem, D.; Kuthan, J.; Ehlert, S. Denial of Service Attacks and SIP Infrastructure: Attack scenarios and prevention mechanisms. *IEEE Netw.* **2006**, *20*, 26–31. [CrossRef]

22. Boro, D.; Basumatary, H.; Goswami, T.; Bhattacharyya, D.K. UDP Flooding Attack Detection Using Information Metric Measure. In Proceedings of the International Conference on ICT for Sustainable Development, Amsterdam, The Netherlands, 29 August–1 September 2016; pp. 143–153.
23. Vennila, G.; Manikandan, M.S.K. A Scalable Detection Technique for Real-time Transport Protocol (RTP) Flooding Attacks in VoIP Network. *Procedia Comput. Sci.* **2016**, *93*, 893–901. [CrossRef]
24. Gao, Y.; Feng, Y.; Kawamoto, J.; Sakurai, K. A Machine Learning Based Approach for Detecting DRDoS Attacks and Its Performance Evaluation. In Proceedings of the 2016 11th Asia Joint Conference on Information Security (AsiaJCIS), Fukuoka, Japan, 4–5 August 2016; pp. 80–86.
25. Rebahi, Y.; Nassar, M.; Magedanz, T.; Festor, O. A survey on fraud and service misuse in voice over IP (VoIP) networks. *Inf. Secur. Tech. Rep.* **2011**, *16*, 12–19. [CrossRef]
26. Vennila, G.; Shalini, N.S.; Manikandan, M. Performance analysis of VoIP spoofing attacks using classification algorithms. In Proceedings of the 2014 Applications and Innovations in Mobile Computing (AIMoC), Kolkata, India, 27 February–1 March 2014; pp. 193–198.
27. Garcia-Teodoro, P.; Diaz-Verdejo, J.; Macia-Fernandez, G.; Vazquez, E. Anomaly-based network intrusion detection: Techniques, systems and challenges. *Comput. Secur.* **2009**, *28*, 18–28. [CrossRef]
28. Fachkha, C.; Debbabi, M. Darknet as a Source of Cyber Intelligence: Survey, Taxonomy, and Characterization. *IEEE Commun. Surv. Tutor.* **2016**, *18*, 1197–1227. [CrossRef]
29. Liu, C.; Xiong, G.; Liu, J.; Gou, G. Detect the reflection amplification attack based on UDP protocol. In Proceedings of the 2015 10th International Conference on Communications and Networking in China (ChinaCom), Shanghai, China, 15–17 August 2015; pp. 260–265.
30. Tariq, U.; Malik, Y.; Abdulrazak, B. Defense and Monitoring Model for Distributed Denial of Service Attacks. *Procedia Comput. Sci.* **2012**, *10*, 1052–1056. [CrossRef]
31. Mirkovic, J.; Reiher, P. A taxonomy of DDoS attack and DDoS defense mechanisms. *ACM SIGCOMM Comput. Commun. Rev.* **2004**, *34*, 39–53. [CrossRef]
32. Angrisani, L.; Moriello, R.S.L.; Lelio, M.D.; Morabito, P.; Vadursi, M. Design and implementation of a reconfigurable test-bed for real-time security measurements in VoIP systems. *Measurement* **2013**, *46*, 3691–3700. [CrossRef]
33. Farley, R.; Wang, X. Exploiting VoIP softphone vulnerabilities to disable host computers: Attacks and mitigation. *Int. J. Crit. Infrastruct. Prot.* **2014**, *7*, 141–154. [CrossRef]
34. Dantu, R.; Fahmy, S.; Schulzrinne, H.; Cangussu, J. Issues and challenges in securing VoIP. *Comput. Secur.* **2009**, *28*, 743–753. [CrossRef]
35. Ehlert, S.; Wang, C.; Magedanz, T.; Sisalem, D. Specification-Based Denial-of-Service Detection for SIP Voice-over-IP Networks. In Proceedings of the 2008 The Third International Conference on Internet Monitoring and Protection, Bucharest, Romania, 29 June–5 July 2008; pp. 59–66.
36. Ehlert, S.; Geneiatakis, D.; Magedanz, T. Survey of network security systems to counter SIP-based denial-of-service attacks. *Comput. Secur.* **2010**, *29*, 225–243. [CrossRef]
37. Hussain, I.; Nait-Abdesselam, F. Strategy based proxy to secure user agent from flooding attack in SIP. In Proceedings of the 2011 7th International Wireless Communications and Mobile Computing Conference, Istanbul, Turkey, 4–8 July 2011; pp. 430–435.
38. Hussain, I.; Djahel, S.; Zhang, Z.; Nait-Abdesselam, F. A comprehensive study of flooding attack consequences and countermeasures in session initiation protocol (SIP). *Secur. Commun. Netw.* **2015**, *8*, 4436–4451. [CrossRef]
39. Wei, W.; Chen, F.; Xia, Y.; Jin, G. A Rank Correlation Based Detection against Distributed Reflection DoS Attacks. *IEEE Commun. Lett.* **2013**, *17*, 173–175. [CrossRef]
40. Tan, Z.; Jamdagni, A.; He, X.; Nanda, P.; Liu, R.P. A System for Denial-of-Service Attack Detection Based on Multivariate Correlation Analysis. *IEEE Trans. Parallel Distrib. Syst.* **2014**, *25*, 447–456.
41. Semerci, M.; Cemgil, A.; Sankur, B. An Intelligent Cyber Security System Against DDoS Attacks in SIP Networks. *Comput. Netw.* **2018**, *136*, 137–154. [CrossRef]
42. Zargar, S.T.; Joshi, J.; Tipper, D. A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks. *IEEE Commun. Surv. Tutor.* **2013**, *15*, 2046–2069. [CrossRef]
43. Dassouki, K.; Safa, H.; Nassar, M.; Hijazi, A. Protecting from Cloud-based SIP flooding attacks by leveraging temporal and structural fingerprints. *Comput. Secur.* **2017**, *70*, 618–633. [CrossRef]
44. Shah, Z.; Ullah, I.; Li, H.; Levula, A.; Khurshid, K. Blockchain Based Solutions to Mitigate Distributed Denial of Service (DDoS) Attacks in the Internet of Things (IoT): A Survey. *Sensors* **2022**, *22*, 1094. [CrossRef]
45. Kurt, B.; Yildiz, C.; Ceritli, T.Y.; Sankur, B.; Cemgil, A.T. A Bayesian change point model for detecting SIP-based DDoS attacks. *Digit. Signal Process.* **2018**, *77*, 48–62. [CrossRef]
46. Tang, J.; Cheng, Y.; Hao, Y.; Song, W. SIP Flooding Attack Detection with a Multi-Dimensional Sketch Design. *IEEE Trans. Dependable Secur. Comput.* **2014**, *11*, 582–595. [CrossRef]
47. Nazih, W.; Hifny, Y.; Elkilani, W.S.; Dhahri, H.; Abdelkader, T. Countering DDoS Attacks in SIP Based VoIP Networks Using Recurrent Neural Networks. *Sensors* **2020**, *20*, 5875. [CrossRef]
48. Amalou, W.; Mehdi, M. An Approach to Mitigate DDoS Attacks on SIP Based VoIP. *Eng. Proc.* **2022**, *14*, 6.

49. Xu, R.; Cheng, J.; Wang, F.; Tang, X.; Xu, J. A DRDoS Detection and Defense Method Based on Deep Forest in the Big Data Environment. *Symmetry* **2019**, *11*, 78. [CrossRef]
50. Nazih, W.; Elkilani, W.S.; Dhahri, H.; Abdelkader, T. Survey of Countering DoS/DDoS Attacks on SIP Based VoIP Networks. *Electronics* **2020**, *9*, 1827. [CrossRef]
51. Keshariya, A.; Foukia, N. DDoS Defense Mechanisms: A New Taxonomy. In Proceedings of the Data Privacy Management and Autonomous Spontaneous Security, St. Malo, France, 24–25 September 2009; pp. 222–236.
52. Tas, I.M.; Tas, H.; Oz, H.B. Cracking the SIP Authentication with a Hybrid Password Cracking Method Specified for SIP Applications. 2014. Available online: https://web.archive.org/web/20220709111334if_/http://www.satee.uab.ro/upls/volum_SATEE_2014.pdf#page=91&zoom=100,45,73 (accessed on 28 November 2022).
53. Zoiper SIP Client (Softphone). 2017. Available online: http://www.zoiper.com (accessed on 25 January 2023).
54. X-Lite SIP Client (Softphone). 2017. Available online: https://www.counterpath.com/x-lite/ (accessed on 25 January 2023).
55. Sassani, B.A.; Abarro, C.; Pitton, I.; Young, C.; Mehdipour, F. Analysis of NTP DRDoS attacks' performance effects and mitigation techniques. In Proceedings of the 2016 14th Annual Conference on Privacy, Security and Trust (PST), Auckland, New Zealand, 12–14 December 2016; pp. 421–427.
56. Liu, B.; Berg, S.; Li, J.; Wei, T.; Zhang, C.; Han, X. The store-and-flood distributed reflective denial of service attack. In Proceedings of the 2014 23rd International Conference on Computer Communication and Networks (ICCCN), Shanghai, China, 4–7 August 2014; pp. 1–8.
57. Ben-Porat, U.; Bremler-Barr, A.; Levy, H. Vulnerability of Network Mechanisms to Sophisticated DDoS Attacks. *IEEE Trans. Comput.* **2013**, *62*, 1031–1043. [CrossRef]
58. Mirkovic, J.; Prier, G.; Reiher, P. Source-end DDoS defense. In Proceedings of the Second IEEE International Symposium on Network Computing and Applications, NCA 2003, Cambridge, MA, USA, 16–18 April 2003; pp. 171–178.
59. Yaar, A.; Perrig, A.; Song, D. StackPi: New Packet Marking and Filtering Mechanisms for DDoS and IP Spoofing Defense. *IEEE J. Sel. Areas Commun.* **2006**, *24*, 1853–1863. [CrossRef]
60. Bermudez-Edo, M.; Salazar-Hernandez, R.; Diaz-Verdejo, J.; Garcia-Teodoro, P. Proposals on assessment environments for anomaly-based network intrusion detection system. *Crit. Inf. Infrastruct. Secur.* **2006**, *LNCS 4347*, 210–221.
61. Rosenberg, J.; Schulzrinne, H.; Camarillo, G.; Johnston, A.; Peterson, J.; Sparks, R.; Handley, M.; Schooler, E. SIP: Session Initiation Protocol. 2002. Available online: https://tools.ietf.org/html/rfc3261 (accessed on 25 January 2023).
62. Wang, H.; Jin, C.; Shin, K.G. Defense Against Spoofed IP Traffic Using Hop-Count Filtering. *IEEE ACM Trans. Netw.* **2007**, *15*, 40–53. [CrossRef]
63. Pereira, D.; Oliveira, R. Detection of Abnormal SIP Signaling Patterns: A Deep Learning Comparison. *Computers* **2022**, *11*, 27. [CrossRef]
64. Lansky, J.; Ali, S.; Mohammadi, M.; Majeed, M.K.; Karim, S.H.T.; Rashidi, S.; Hossein, M.; Rahmani, A.M. Deep Learning-Based Intrusion Detection Systems: A Systematic Review. *IEEE Access* **2021**, *9*, 101574–101599. [CrossRef]
65. Charmet, F.; Tanuwidjaja, H.C.; Ayoubi, S.; Giemenez, P.; Han, Y.; Jmila, H.; Blanc, G.; Takahashi, T.; Zhang, Z. Explainable artificial intelligence for cybersecurity: A literature survey. *Ann. Telecommun.* **2022**, *77*, 789–812. [CrossRef]
66. Capuana, N.; Fenza, G.; Loia, V.; Stanzione, C. Explainable Artificial Intelligence in Cybersecurity: A Survey. *IEEE Access* **2022**, *10*, 93575–93600. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.