electronics

MDPI

Article

Survey of Countering DoS/DDoS Attacks on SIP Based VoIP Networks

Waleed Nazih [1,2,*], Wail S. Elkilani [2,3], Habib Dhahri [3,4] and Tamer Abdelkader [2]

[1] College of Computer Engineering and Sciences, Prince Sattam Bin Abdulaziz University, Al Kharj 11942, Saudi Arabia
[2] Faculty of Computers and Information Sciences, Ain Shams University, Abassia, Cairo 11566, Egypt; welkilani@ksu.edu.sa (W.S.E.); tammabde@cis.asu.edu.eg (T.A.)
[3] College of Applied Computer Sciences (CACS), King Saud University, Riyadh 11543, Saudi Arabia; hdhahri@ksu.edu.sa
[4] Faculty of Sciences and Technology, University of Kairouan, Sidi Bouzid 4352, Tunisia
* Correspondence: w.nazeeh@psau.edu.sa

Received: 3 September 2020; Accepted: 27 October 2020; Published: 2 November 2020

Abstract: Voice over IP (VoIP) services hold promise because of their offered features and low cost. Most VoIP networks depend on the Session Initiation Protocol (SIP) to handle signaling functions. The SIP is a text-based protocol that is vulnerable to many attacks. Denial of Service (DoS) and distributed denial of service (DDoS) attacks are the most harmful types of attacks, because they drain VoIP resources and render SIP service unavailable to legitimate users. In this paper, we present recently introduced approaches to detect DoS and DDoS attacks, and classify them based on various factors. We then analyze these approaches according to various characteristics; furthermore, we investigate the main strengths and weaknesses of these approaches. Finally, we provide some remarks for enhancing the surveyed approaches and highlight directions for future research to build effective detection solutions.

Keywords: voice over IP; session initiation protocol; network security; denial of service; distributed denial of service attacks

1. Introduction

Voice over IP (VoIP) is the technology used for transferring voice and multimedia data over Internet Protocol (IP) networks. VoIP systems are taking over traditional solutions worldwide because of their low cost and high quality of service for voice and multimedia communications. VoIP is also expected to become the dominant technology for voice communications with fifth-generation (5G) networks. Recently, many companies and organizations have updated their communication systems to VoIP from traditional telephone systems [1]. The rapid growth of VoIP makes it an attractive target for attackers, which in turn may cause a reduction in quality of service (QoS) [2].

Figure 1 shows VoIP system's primary components namely; end-user equipment, network components, call processors, gateways, and protocols [3].

End-user equipment is used to access the VoIP system and communicates with other endpoints. In addition, it initiates and maintains the necessary signaling process to establish calls over the network. Softphones, phones with IP facilities, and multimedia computers are examples of end-user equipment.

Network components are cables, routers, switches, wireless access points, and firewalls. It is usually the IP network where the VoIP system is installed.

Call processors perform many functions such as call setup, monitoring of calls, and user authorization. A call processor is usually a software running on top of an operating system.

Gateways manage call origination and detection. In addition, they handle analog to digital conversion. VoIP system may have a Media Gateway (MG), a Media Gateway Controller (MGC), and a Signaling Gateway (SG). MG handles streams of media. MGC is responsible for call control. SG acts as an interface with external networks.

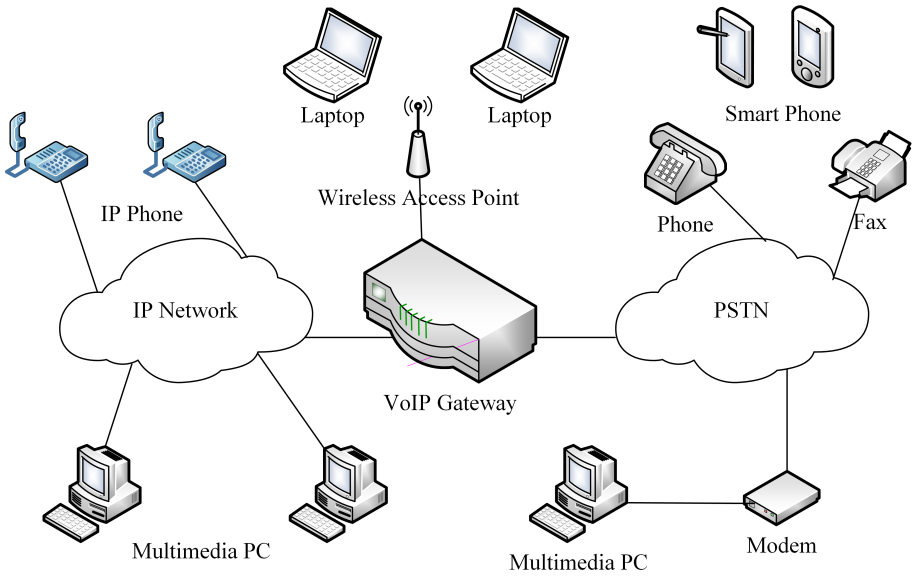

Figure 1. Primary components of the VoIP system.

VoIP systems use data transfer protocols such as the Real-Time Transport Protocol (RTP) [4] to transfer voice and multimedia data over packet-switched IP networks. In addition, they use signaling protocols such as H.323 or the Session Initiation Protocol (SIP) [5] to manage communication sessions. Therefore, VoIP systems are vulnerable to attacks that are generated from two sources: network protocols such as the User Datagram Protocol (UDP) and VoIP specific protocols such as SIP [6]. VoIP specific attacks usually are not detected by network security systems; extra security mechanisms are therefore necessary for VoIP systems to detect and prevent these attacks.

VoIP networks have recently been vulnerable to many security threats. In addition, the intensity of attacks seems to have been growing [7]; this might be a result of the rapid increase in the capabilities of tools used by attackers. Two of the most harmful and specific types of VoIP attacks are denial of service (DoS) and distributed DoS (DDoS). The main objective of these attacks is to prevent legitimate users from using VoIP services. These attacks may affect VoIP service availability by targeting one or many VoIP servers [8]. Such attacks can thus affect business productivity and lead to revenue loss.

As a matter of fact, the survey presented in this paper introduces an up-to-date survey of DoS and DDoS attacks detection approaches over VoIP networks. The novelty of our survey compared to previously cited surveys is the way it tackles with the proposed approaches in the literature. It gives a thorough in-depth analysis of these approaches with respect to different factors. Hence, robust and flawed aspects are enlightened. This is very important for complex problems where we need to pick out a suitable technique, which effectively reduced time and cost. Actually, the survey is motivated by the challenges faced by the VoIP security community. Several of these challenges are resolved by the analysis given through a number of comparison tables. Open research topics are concluded based on these challenges. The mentioned research directions constitute a distinguished motivation for the survey.

Obviously, we can summarize the survey contributions as (1) introducing up-to-date detection approaches for DoS and DDoS attacks; (2) analyzing the proposed approaches according to the most important factors, such as the types of attacks detected; (3) identifying strengths and weaknesses of the proposed approaches; and (4) Determining open challenges to achieve effective detection of DoS and DDoS attacks regarding VoIP systems. The rest of the paper is organized as follows. Section 2

summarizes the related work. In Section 3, we introduce SIP and its main components. DoS and DDoS attacks are explained in Section 4. The surveyed approaches are overviewed in Section 5. The analysis and comparison of the surveyed approaches are presented in Section 6. Open challenges that require further attention and future aims of our research are discussed in Section 7. Finally, Section 8 concludes the paper.

2. Related Work

Many surveys tackle different aspects of network security, such as [9,10]. VoIP security has been extensively investigated in recent years. However, most of these studies are generic and have focused on many types of VoIP attacks. For example, a comprehensive survey of VoIP vulnerabilities and security approaches based on a critical review of 245 publications was presented in [6]. In this study, a comparison of DoS vulnerabilities was performed along with the possible approaches to reduce VoIP DoS attacks. It was found that little research (less than 13%) focus on DoS attacks; significantly more work is needed.

Other surveys focused on a specific type of VoIP attacks such as spam over Internet telephony (SPIT). Azad et al. [11] discussed detecting and mitigating SPIT and spamming in VoIP networks. In addition, they highlighted the challenges in developing SPIT and spamming detection systems. Finally, the shortcomings of existing solutions and future research directions were outlined. Naeem et al. [12] provided a thorough analysis of the SIP's registration attack. They categorized the surveyed solutions based on their approaches, targets, and types. They also conducted robustness and inefficiency tests, as well as basic assumptions computations of these solutions to discover its limitations. Finally, they suggested using the media access control (MAC) to protect the user agent client (UAC) registration method against the registration attack.

With regards to surveys on DoS and DDoS attacks, a review of SIP malformed messages found in DoS attacks was presented in [13]; the authors listed the types of malformed messages. Moreover, they analyzed four articles and evaluated them according to their advantages and limitations. Hussain et al. [14] introduced a comprehensive study of SIP flooding DoS attacks. They classified the research work reviewed (consisting of 26 publications) according to attack behavior, attack type (internal or external), and attack target (proxy server or end-user). Furthermore, they highlighted the strengths and weaknesses of the reviewed solutions and provided some recommendations of enhancement for the surveyed solutions. Ganesh et al. [15] surveyed 15 publications of DoS attacks. They categorized these papers according to the attack method and prevention mechanisms.

DoS and DDoS attack detection frameworks were reviewed in [16]. The authors chose eight frameworks and conducted a comparison between them. Furthermore, they suggested evaluation criteria, called DADMV, for evaluating these frameworks. DADMV consists of five groups: Depiction, Architecture, Detection, Mitigation, and Validation. Each group consists of a set of parameters used to evaluate the revised frameworks. For example, the validation group checks the framework's bandwidth scalability, memory and CPU usage, financial cost, and its applicability. In Table 1, we present a brief comparison between our survey and the other mentioned surveys.

From the previous discussion, it can be noted that published surveys are either limited in their scope to a specific type of DoS attacks [13,14] or examined them with limited aspects of comparison [15] or did not provide a review of the recently published articles [16]. Hence there is a need for a recent and in-depth survey. Our paper's major contribution, based on previous work, is that it introduces a deep investigation of recent approaches used for DoS and DDoS detection. We have reviewed as many as we could find of the articles that were published between 2014 and the first half of 2020 (28 articles). In addition, we have analyzed these approaches based on many factors and also have introduced a comparison of the strengths and weaknesses of each.

Table 1. Comparison between our survey and recent surveys. SPIT, spam over Internet telephony.

Reference	Covered Papers	Covered Period	Attacks	Comparison Criteria
[11]	65	2004–2018	SPIT and Spamming	Not mentioned.
[12]	26	2014–2019	Registration Hijacking	Detected hijacking attacks, attack type, attack targets, validation mechanism, registration hijacking approach, detection approach, important aspects, and assumptions.
[13]	4	2007–2015	Malformed Messages	Detection approach, advantages, and limitations.
[14]	26	2004–2015	Flooding	Attack behavior, attack type, attack target, attack source, validation, strengths, weaknesses, and assumptions.
[15]	15	2006–2010	DoS	Attack method and prevention mechanism.
[16]	8	2007–2013	DoS and DDoS	Depiction, architecture, detection, mitigation, and validation.
This survey	28	2014–2020	DoS and DDoS	Detection approach, detected attacks, detection time, performance, strengths, and weaknesses.

3. SIP Overview

VoIP services use the H.323 and SIP protocols for audio and visual communication. Even though both SIP and H.323 provide similar capabilities, SIP is the dominant signaling protocol used for VoIP because of its simplicity, easy implementation, and lightweight operation.

SIP is an application layer protocol that is responsible for creating, modifying, and terminating communication sessions. It also performs signaling functions for clients' registration and availability checks. Moreover, SIP can be integrated with other protocols such as the Session Description Protocol (SDP) [17].

3.1. Architecture

The main components of SIP architecture are depicted in Figure 2. The logical endpoints in SIP network are end-user devices called user agents (UAs). The UA is a network element that can create, send, receive, and process SIP messages. During a SIP session, the UA can act as a client (the user agent client or UAC) or act as a server (the User Agent Server or UAS). The UAC sends SIP requests, while the UAS receives them and generates the appropriate SIP responses. The UA is either a hardware-based or software-based SIP phone. Finally, the uniform resource identifier (URI) is used for identification purposes; each UA has a unique identifier.

SIP can be used without central servers (i.e., peer to peer); however, this is not practical for large deployments. To deal with this, SIP has defined the following elements: the proxy server, the registrar, and the redirect server.

The proxy server manages the setup phase of the SIP call. It is responsible for registration, call routing, authorization, and network access. Therefore, all calls pass through this server at first. Moreover, it routes the requests to the user's location. Finally, it implements different policies that are set by the service provider.

The registrar stores SIP URI and IP address information. It is usually connected to the proxy server and sometimes connected to the redirect server.

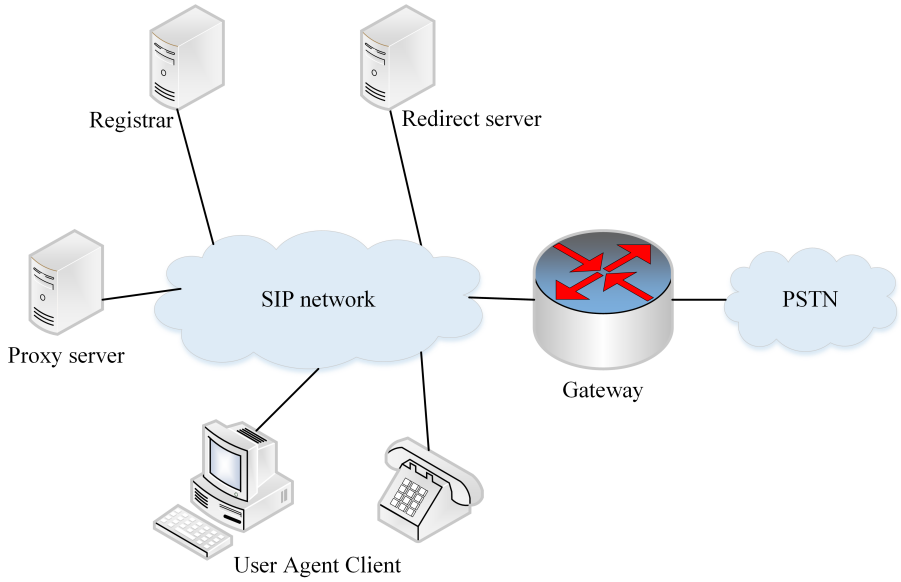

Figure 2. Main components of SIP architecture.

The redirect server plays a central role in the SIP network. It performs tasks such as redirecting traffic to alternative SIP URIs upon receiving a redirection message and connecting the proxy server to external domains. Sometimes, it is used to decrease the proxy server's processing load. Furthermore, the redirect server forwards request routing information to the desired destination if the SIP server is not responding to a client's request. The previous servers are usually implemented over one server called the SIP server.

Finally, the SIP architecture may have other network elements acting as general gateways. The main function of these gateways is to provide a connection with other types of networks such as mobile networks and the public switched telephone network (PSTN).

3.2. Call Establishment

Establishing the SIP call is a simple process, as shown in Figure 3. The process begins with the calling party sending a SIP INVITE message to the called party; this message is an invitation to the called party to participate in a session or a call. Second, the called party can respond to the invitation by issuing different responses before accepting it. In some cases, it might inform the caller that the call is being queued or that the called party is being alerted. After the called party answers, an OK response is sent to the caller; the caller then replies with an ACK message. At this point, both parties can start exchanging messages, which can be in voice or video format.

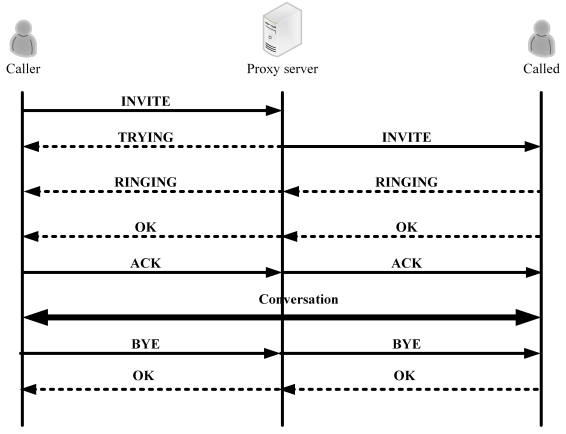

Figure 3. Session Initiation Protocol (SIP) call establishment.

Finally, when one party decides to end the call, it sends a BYE message to the second party, which then responds by sending an OK message to confirm the receipt of the BYE message.

3.3. Messages

SIP messages are categorized into requests and responses. The standard process of message exchange starts with a request from the UAC to the UAS. Then, the UAS processes this request and replies with an appropriate response. Finally, the UAC processes the received response and may continue by generating a new request. Every SIP message has a header and body. The header contains additional information about the request or response, while the body describes the type of session to be established.

3.3.1. Requests

The first line of each SIP request contains the request type, the URI, and the SIP version. The rest of the header contains additional information such as the contacting party and a description of the message contents. Below is an example of a SIP request.

```
INVITE sip: Bot67@kankuro SIP/2.0
Call-ID: a5cb7d37f858feddbe9aa8ef9163e09e@192.168.1.13
CSeq: 1 INVITE
From: "Bot9" <sip:Bot9@192.168.1.13>; tag = 920
To: <sip: Bot67@kankuro>
Via: SIP/2.0/UDP 192.168.1.13:5079; branch = z9hG4bK03dfd97c4e6b09451a0c09806737f39e
Max-Forwards: 70
Contact: <sip: Bot9@192.168.1.13:5079>
User-Agent: Twinkle-v1.1
Content-Type: application/sdp
Content-Length: 250
```

Each SIP server must implement six basic requests; eight optional requests can be implemented as an extension [5]. The six basic requests are INVITE, ACK, BYE, OPTIONS, CANCEL, and REGISTER.

- INVITE: starts SIP session
- ACK: confirms the receipt of the final response
- BYE: terminates SIP session
- OPTIONS: queries SIP server capabilities
- CANCEL: terminates pending requests
- REGISTER: registers the UA address with the SIP server

3.3.2. Responses

The SIP response starts with a status line that contains the SIP version, status code, and reason phrase (for example, SIP/2.0 200 OK). Reason phrases are made short to be understandable, and the status code has values between 100 and 699 with the first digit indicating the response class: 1XX for provisional, 2XX for success, 3XX for redirection, 4XX for request failure, 5XX for server failure, and 6XX for global failure. Each response code has a corresponding response phrase. For example, the 401 code is used when the client is not allowed to perform a request; It is one of the 4xx codes, and has the phrase "Unauthorized".

4. DoS and DDoS Attacks on SIP

VoIP networks are vulnerable to many attacks [6]. The full classification of these attacks was explored in [18]. In this section, we explore DoS and DDoS attacks.

4.1. Denial of Service Attacks

Any attack that makes a target SIP service or resource unavailable to legitimate users is a DoS attack. The attacker usually targets the SIP server to prevent subscribers from using VoIP services or degrading the quality of offered services. The most common DoS attacks are flooding and malformed messages.

4.1.1. Flooding Attacks

These attacks are based on generating a large number of SIP messages to force the SIP client or server to consume its resources (e.g., memory and CPU). Therefore, the SIP component will be put out of service for legitimate users. This attack has multiple forms such as INVITE flooding, shown in Figure 4, REGISTER flooding, BYE flooding, and multi-attribute flooding [19].

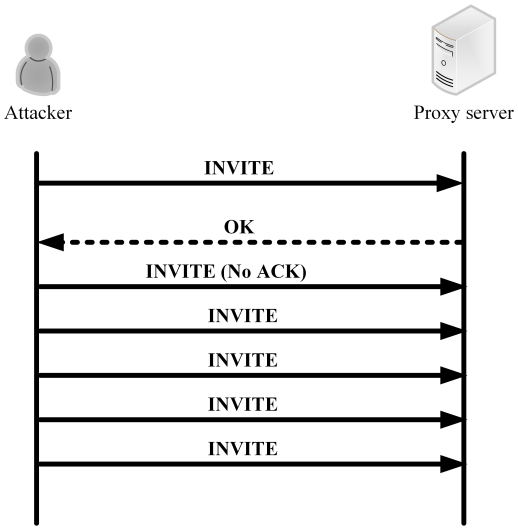

Figure 4. An INVITE flooding attack.

4.1.2. Malformed Message Attacks

The attacker modifies a correct SIP message, which then causes a partial failure or a reboot of the SIP component (i.e., the SIP client or server) when an attempt is made to process this message. Any SIP message that is incompatible with the correct SIP syntax [5] is considered to be a malformed message. Because the SIP component's parser was written to process correctly formatted SIP messages, there are a large number of SIP messages that will be considered syntactically incorrect.

Finally, a malformed message can take many forms, for example with an invalid method name, a disarrangement in message hierarchy, or a missing mandatory SIP header. The SIP-Msg-Gen tool [20] can generate malformed messages using many different scenarios. Below is an example of a malformed message - with an invalid method name—that was generated by this tool.

```
8rafgki sip: xzmLqOZp@WD.22mSIlpi.bb SIP/2.0
CSeq : 0 OPTIONS
Via: SIP/2.0/UDP pc77.atlanta.com; branch = z9hG4bK336asdhds; received = 192.0.2.5
To: sip:xzmLqOZp@WD.22mSIlpi.bb; tag = U7IZWSXQ
Max-Forwards: 242
From: sip: xjlE@rCRzWf.M6ilfPsE.bs; tag = L5EgPZ1wQ
Contact: "Mr. Bill" <sip:bill@worcester.bell-telephone.com>; q = 0.7; expires = 3600
Call-ID: YeZ8Dao18g1tSj@ZtHRcJSjOXjqeL
Accept: application/sdp; level = 3, application/x-private, text/html
Content-Language: EbxqOZGc
Content-Type: application/sdp
Content-Length: 40
Date: Wed, 28 Sep 2012 23:29:00 GMT
v = 0
o = mhandley 29739 7272939 IN IP4 126.5.5.3
c = IN IP4 135.180.130.85
t = 0 0
m = audio 492170 RTP/AVP 0 12
s = 1
a = rtpmap : 31 LPC
```

4.2. Distributed Denial of Service Attacks

A DDoS attack is a DoS attack performed using many computers simultaneously. These attacks are always produced using a group of computers controlled by the attacker (i.e., botnet). The attacker infects computers of compromised users through a worm used to control and exploit their computers in a DDoS attack [21]. Detecting DDoS attacks is more complicated than DoS attacks because source blocking based on traffic limitations is useless. Furthermore, compromised users are usually unaware that their computers are a part of a DDoS attack.

5. Recent Approaches

The surveyed approaches to protecting VoIP networks from DoS and DDoS attacks are classified as shown in Figure 5. The existing approaches can be categorized into four types: finite state machine (FSM) approaches, rules-based approaches, statistically based approaches, and machine learning approaches.

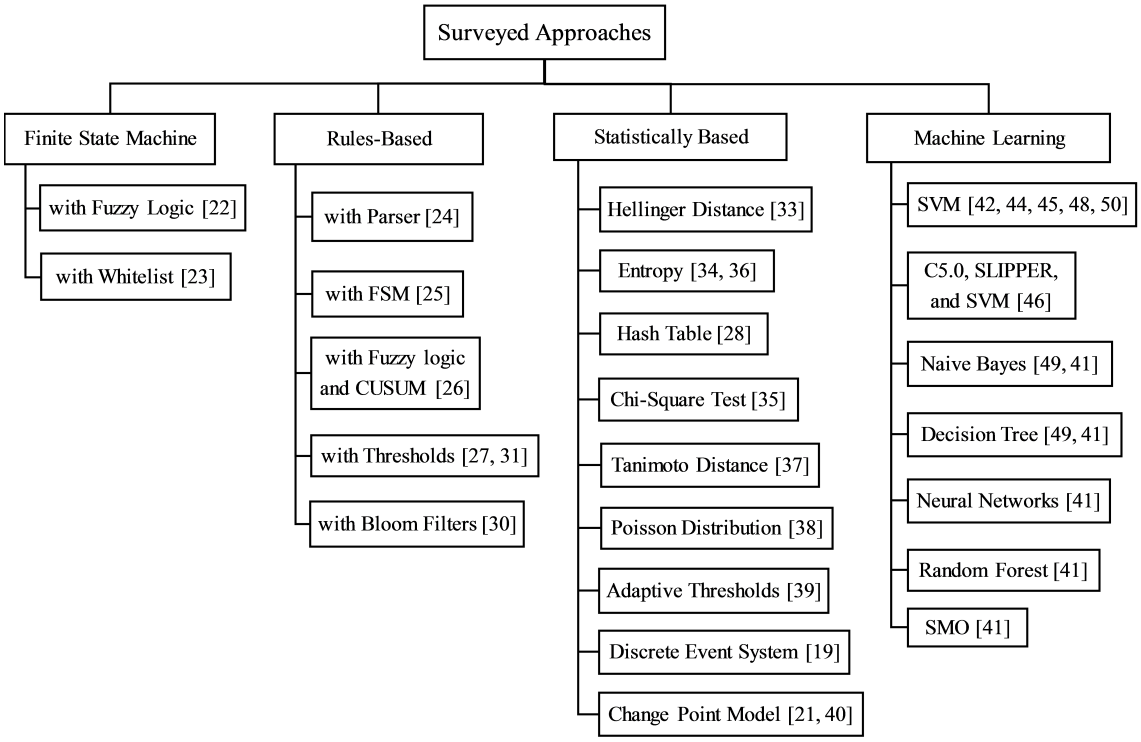

Figure 5. Classification of surveyed approaches.

5.1. Finite State Machine Approaches

The SIP state machine is tracked, and the system raises an alarm if any deviation from the expected state transition is found. Implementing an FSM for SIP requires a well thought out design and is usually coupled with a whitelist to store normal messages or legitimate user data. A whitelist entry may be a "From" and "To" SIP address, or the source and destination IP addresses.

Hosseinpour et al. [22] used normal SIP calls to create an FSM. The number of messages in state transitions were calculated during the day, and an average of time differences between FSM states was extracted. For flooding attack detection, fuzzy logic is used to determine the attack severity at the end of a time interval. By using call detail records (CDRs), users who finish their calls successfully are added to the whitelist; only whitelisted users can reach the server while in the attack state. They achieved a low false alarm ratio by using proper time intervals and by tuning the fuzzy system.

The proposed approach in [23] used the temporal features of the SIP state machine and SIP message databases containing IP-fingerprints to detect and mitigate flooding attacks. The state machine handles each SIP session and generates some events. Then, a detector uses the generated events to classify SIP sessions as normal or abnormal and stores the session IP-fingerprint in the databases accordingly.

A filter module allows a normal message to reach its destination; the mitigation process is started for an abnormal message. Moreover, the design of the proposed approach takes into consideration the attack intensity and uses a less restrictive whitelist algorithm that requires relatively little in terms of computational resources. Sources of attack deployed on different sites and real cloud scenarios were used to test the systems against low and high-rate flooding attacks as well as DDoS. The results reported a reduction in computational resources used and short detection times when compared to other approaches cited in their literature.

5.2. Rules Based Approaches

A set of rules is used to decide whether a SIP message is normal or malicious according to certain characteristics. Such approaches require a thorough knowledge of SIP, threshold fine-tuning, and manual work to design and regularly update the rules. The main defect of these rules-based approaches is their failure to detect new attacks if the corresponding rules are not updated.

Recently, Tsiatsikas et al. [24] found that the previous work cited in their literature tended to focus on information extracted from only the headers of SIP messages. Consequently, they built a parser, based on the SDP, to detect malformed message attacks exploiting the SIP message body. This parser contains 100 different rules to make sure that the body of the SIP message is correct according to SDP syntax. High accuracy was achieved with little processing time overhead.

A detection approach implemented at the SIP data plan level was proposed in [25]. This approach deploys distributed SIP sensors at every switch and server, which enables the isolation of damage at a specific switch. After tracking the SIP finite state machine to determine the maximum number of INVITE packets per port, a group of rules was created to drop INVITE packets if the limit was exceeded. An experiment has been performed to detect INVITE flooding attack when the attacker sent 10,000,000 INVITE packets; the system considered only the first INVITE packet as normal, and the remaining packets were detected as malicious.

Sun et al. [26] proposed a SIP flooding attack detection scheme (SFADS) to detect low-rate and high-rate flooding attacks. They used the number of INVITE messages and the SIP session establishment sequence as detection features. Moreover, the improved cumulative sum control chart algorithm (CUSUM) analyzed these features, and fuzzy logic with 25 rules takes the analysis data as input and produces the detection decision as output. SFADS was found to outperform CUSUM schemes in terms of false alarm ratios and detection times.

Cadet et al. [27] proposed a system that integrated the rules of [28] with Snort [29] in inline mode. They deployed Snort as an intrusion prevention system to drop suspicious messages. Experiments over one minute were performed with different attack rates, and the proposed approach detected high-rate INVITE flooding in 500 ms. In addition, the SIP server's memory and bandwidth were saved from any consumption that would occur as a result of an attack. To detect stealthy attacks, the system rules should be modified.

Ganesan et al. [30] proposed a two phased model to detect flooding and fake signaling attacks. Four SIP attributes (i.e., To URI, From URI, and source and destination IP) were extracted from every SIP session between the same users in the same direction; these attributes were used as an index for the sessions database and as an input for the second phase. In the first phase, a set of pre-defined rules were applied to either drop or forward a message to the second phase. A modified Bloom filter and a set of hash functions were used in the second phase to prevent attacks, and any message deemed as part of an attack would be added to a blacklist. Using six hash functions, the proposed approach achieved high detection accuracy, albeit with a high detection time (9 s for INVITE flooding attacks, and 12 s for fake signaling attacks).

Tas et al. [31] investigated the vulnerabilities of SIP and reported two advanced DDoS attacks that can exploit IP spoofing techniques. Then, they proposed a two-module mechanism to protect the SIP server from these attacks. A statistics module calculates traffic statistics (i.e., dynamic threshold) over a period of time, then a rules-based action module used the previously calculated thresholds to take suitable action. Moreover, they developed a DDoS attack simulator to test for the reported attacks and proposed mechanism. Finally, they showed that the proposed mechanism reduced the CPU processing of the SIP server under attack by 73.4%; however, they did not calculate detection accuracy against DDoS attacks. In [32], they introduced a new SIP-based Distributed Reflection Denial of Service (SR-DRDoS) attack. This attack exploits some of the SIP features using IP spoofing mechanism and logic of reflection based and DDoS attacks. Actually, it increased the SIP server's CPU load to 100% in four minutes. They proposed a defense mechanism that collected a window of network traffic

periodically. Hence, a group of thresholds was calculated which in turn triggers rule-based filtering actions. This mechanism succeeded to reduce the CPU load of the SIP server under attack.

5.3. Statistically Based Approaches

A statistical or mathematical model is built in the training phase to describe normal behavior for SIP sessions. Then, if incoming SIP messages have significant deviation—usually by exceeding some threshold(s)—from normal behavior, an attack alarm is raised. Because these approaches are sometimes based on the differences in occurrence counts of different events, it may fail to detect certain attacks or produce false alarms [19]. These can automatically detect unknown attacks in the meantime.

A firewall module using a multi-dimensional sketch and Hellinger distance (HD) was proposed in [33]. SIP messages were converted to a probability distribution over the sketch table by using a three-dimensional sketch that stores every SIP attribute (INVITE, OK, ACK, BYE) and its hash functions. The HD value was used as an anomaly indicator; a high value of HD means a large deviation in SIP traffic and signifies that an anomaly has occurred, while a low value means no change in SIP traffic. The proposed approach was tested against DoS flooding, and achieved promising results with DDoS attacks; however, it cannot detect stealthy flooding attacks.

A similar approach that used Shannon entropy instead of HD for network traffic behavior analysis was proposed in [34]. They started with network traffic, free from attack, to create the required sketch table, and calculated the entropy over this structure to use as a comparison reference. The difference between the entropy of the testing interval and training interval was checked by a threshold; if this difference is larger than the threshold, a flooding attack is detected. Otherwise, the system will move forward as a sliding window into network traffic and adjust training and testing intervals. They evaluated the proposed system with several flooding scenarios and calculated the detection probability and the false alarm rate for every experiment.

A mitigation scheme based on detailed SIP call analysis was introduced in [28]. INVITE and BYE messages were counted to discriminate between malicious and legitimate users. A hash table stores entries of every call and a counter was incremented with INVITE messages and decremented with BYE or CANCEL messages. They implemented this scheme on the Asterisk SIP server but did not measure its accuracy. Using a static threshold and modifying the SIP proxy server are serious drawbacks of this approach.

Using string comparison and Chi-squared tests, Su et al. [35] proposed the detection of malformed messages and flooding attacks. String comparison based on the principles presented in [5] was used to check if a SIP message is malformed or normal. If the message is normal, the Chi-squared test was calculated over the 10 features of a SIP message, and pre-calculated thresholds were used to determine whether the SIP server is under flooding attack or not. Once a malformed message or a flooding attack is detected, the SIP server blacklist is updated to prevent further messages from the user of the originating message. The malformed messages detection module achieved 0 False Positive (FP) and 1.6–4.8% False Negative (FN), but the Chi-squared calculations consumed system resources and time.

Tsiatsikas et al. [36] used VoIP audit trails, which were found to contain much useful information. In the beginning, they anonymized log files to hide user information. Many anonymization techniques were analyzed and the hash based message authentication code (HMAC) scheme was deemed to be the best choice. The entropy value, based on some message headers, is computed and compared with reference values (generated from clean or attack-free data), and if the entropy value exceeds a predefined threshold, the message is classified as malicious. Furthermore, a de-anonymization module was developed to enable the service provider to retrieve more information about a malicious message. The detection accuracy was evaluated against many DoS scenarios using FP and FN metrics. Offline detection was more robust than online detection; however, online detection has little processing overhead and is easily adjustable.

Chaisamran et al. [37] proposed an anomaly-based detection system to detect flooding attacks. They used the Tanimoto Distance to determine the correlation between the selected attributes, and the

adaptive threshold to detect a significant deviation of traffic. Moreover, a trust model was integrated with the proposed system to handle the degradation of detection accuracy if legitimate traffic volume was suddenly increased. A trust value for each user was calculated using several parameters such as the call direction and call duration. Because the proposed system performs lightweight calculations and does not store all traffic in memory, it does not consume excessive memory or computing resources. In addition, it achieved high detection accuracy and outperformed the HD and CUSUM approaches in terms of the FP rate.

Golait and Hubballi [38] proposed a voice over IP flooding detection (VoIPFD) approach to detect flooding attacks. They used a Poisson distribution to create a normal SIP traffic profile. This distribution takes the average of SIP events of interest (INVITE, REGISTER, BYE, and multi-attribute flooding) during the time period and over some samples. In the training phase, a threshold probability for each SIP event was calculated. Later, the probability of the count of each SIP event during the time period in the testing phase was calculated, and a flooding attack alarm would be raised if this probability was less than the threshold probability. To keep the system updated with the expected change in SIP normal traffic behavior, the mean of the number of SIP events and the Poisson distribution of the events were updated. Simulated traffic of 38 h duration was collected and divided into training periods of 10 min to evaluate detection accuracy with different attack rates.

Lee at al. [39] proposed a statistics-based module to detect DoS attacks and a call behavior-based module to detect SPAM attacks. First, the statistics-based module analyzed SIP traffic to determine if there was a DoS attack or not. If a DoS attack was detected, the SIP packets are dropped. In the case of normal traffic, the adaptive thresholds are updated, and the second module starts. SIP messages were grouped based on IP, Call-ID, URI, and the request method to generate call establishment statistics. At every time interval, calculated statistics were compared with adaptive thresholds and if these fell outside the range established by the thresholds, an attack was determined to have occurred.

Golait et al. [19] proposed a discrete event system and a new state transition machine for SIP. They modeled different SIP dialogues and transactions and described them using a probabilistic state transition machine. Two types of DoS attacks are considered (i.e., coordinated and flooding attacks). The detection algorithms proposed to detect these attacks are based on the anomalies that can occur in the proposed model (i.e., illegal transitions and timing constraint violations). Experiments with different attacks showed that the proposed system achieved high detection accuracy, outperformed the proposed approach in [39], and had the same accuracy as the random early termination (RET) method.

Using a change-point model for DDoS flooding attacks detection and attacker identification was proposed in [21]. The proposed system monitors Mahalanobis distance changes between successive features vectors in a sampling interval (i.e., 1 to 10 s). If the Mahalanobis distance exceeds a pre-defined threshold, the system labeled this as an attack. Furthermore, to identify the attackers from legitimate users, the system clusters the similarity score of the users' behavioral patterns. Furthermore, the system does not require any additional information and uses only the intensity and type of VoIP traffic. The detection accuracy was low (F1 score: 88%) using a 10 s sampling interval, which is considered a long time for real-time systems to detect an attack.

DDoS flooding attacks detection was proposed by Kurt et al. [40]. They extracted a large number of features (i.e., 41 features) from SIP messages and resource usage measurements of the VoIP server. The extracted features were related to hidden variables using the Hidden Markov Model, and a Bayesian multiple change model used these variables as change-point indicators to detect DDoS flooding attacks. Moreover, the maximum likelihood approach was used to find the best values of the model parameters. To evaluate the proposed approach, a SIP simulator was developed to generate normal messages, and the Nova-VSpy tool was used to generate malicious messages. Good detection accuracy was achieved over many DDoS attacks with different traffic intensities.

5.4. Machine Learning Approaches

Starting with the feature extraction process that converts SIP messages into numeric feature vectors, these feature vectors are used to create a model for recognizing some patterns based on training examples. A machine learning (ML) task usually starts with choosing a suitable algorithm. Second, a training dataset is used to adjust the algorithm parameters. Finally, a test dataset is used to evaluate performance. These approaches have always outperformed previous approaches [41].

Asgharian et al. [42] extracted statistics features from SIP headers over a window of SIP messages. They chose these features based on normal SIP behavior and SIP attack characteristics. In addition, they considered the processing time for these features to be close to real-time. Moreover, the Support Vector Machine (SVM) classifier was used to evaluate the proposed features against REGISTER, RINGING, and INVITE flooding attacks. Finally, their simulated dataset and INRIA dataset [43] were used to evaluate the proposed features. They achieved high detection accuracy but also a high FP rate.

Similarly, Pougajendy et al. [44] extracted two new features (number of first INVITE messages and the number of first ACK messages received by the SIP Server) and a subset of [33,42] other features. The suggested features were calculated and normalized over a buffer of 20 packets, which takes about 2 s. They adjusted the SVM classifier to increase detection accuracy and minimize the false alarm rate. Comparing the proposed classifier with other classifiers such as Decision Tree and Naive Bayes, it achieved comparable results with high-rate flooding attacks and high detection accuracy with low-rate flooding attacks.

Vennila et al. [45] proposed a two-tier model that classifies network traffic into VoIP and non-VoIP using SVM classifier. Then, an entropy model classifies the VoIP traffic into normal and malicious traffic. They used a set of seven features with the SVM classifier and tried the Radial Basis Function (RBF) and the Linear kernels. Moreover, the number of signaling packets was used as a function of entropy, and the maximum and minimum traffic peaks were used to adjust the required thresholds. The proposed model outperformed traditional SVM in their experiments and achieved 95% detection accuracy.

Preventing mimicry telephony denial of service (TDoS) using multiple classifier systems (MCS) was proposed by Marchal et al. [46]. Mimicry TDoS can be launched by a malformed message that is slightly changed from a normal message. To avoid SIP message parsing, an n-gram technique was used to extract features from SIP messages and then choose the 2000 n-gram having the highest frequency count. Moreover, an optimization problem was solved to find the smallest number of classifiers needed to achieve high detection accuracy. Experiments were conducted using real traffic traces from two different sources and 28 classifiers from Weka [47]. The best detection accuracy was achieved using 3 classifiers (C5.0, SLIPPER, and SVM).

Similarly, Nazih et al. [48] used an n-gram technique and a fast linear SVM classifier to detect INVITE flooding, malformed message, and SPIT attacks. First, a window of four characters was moved over the SIP message to extract all n-gram tokens and store in the features vector the number of occurrences for each n-gram. Second, to avoid the main drawback of the traditional dual form SVM, an l_1 regularizer that produces sparse solutions was used with SVM in its primal form. Two different datasets were used to evaluate the l_1-SVM classifier that achieved a high detection rate and low detection time. In addition, l_1-SVM outperformed traditional dual form SVM in detection and training times.

M.Akbar et al. [49] proposed a real-time packet-based SIP intrusion protector (PbSIP) to detect DoS flooding, DDoS flooding, and SPIT attacks. They analyzed the advantages and disadvantages of flow-based and packet-based monitoring and decided to use packet-based monitoring. PbSIP has three modules: a packet analyzer module that monitors packets of the SIP traffic, a feature extraction module that calculates spatial and temporal features over a window of 40 packets, and a classification module that uses Naive Bayes to classify messages as normal or malicious. They tested PbSIP over a set of different intensity attack scenarios; PbSIP outperformed HD and SVM in detection accuracy and processing overhead.

Tsiatsikas et al. [41] argued that ML can be used to examine high volumes of offline VoIP log files and can achieve better detection accuracy in the case of low-rate DoS attacks. First, they calculated the occurrences of 6 mandatory SIP headers for a window of messages (i.e., 1000 messages) in the feature extraction phase. Second, five classifiers (neural networks, naive Bayes, random forest, decision trees, and sequential minimal optimization (SMO)) were applied over 15 different DoS and DDoS scenarios in the classification phase. Furthermore, HMAC anonymization was used over SIP headers to preserve user privacy. For DDoS scenarios, the proposed classifiers outperformed the Entropy, and Hellinger Distance approaches in terms of FN. In addition, the FP percentages for DDoS scenarios were higher than those obtained in the case of the DoS scenarios.

Akbar et al. [50] proposed a SIP parser to detect malformed message DoS attacks. The proposed system starts with a lexical analyzer that converts SIP message to lexemes, stores them in a table, and discards the syntactically incorrect messages. Later, SVM classifies the syntactically correct SIP messages into normal or malformed message. Moreover, kernel tree analysis was used to reduce the processing time because it does not require feature space representation. A dataset of 5000 SIP messages (500 normal messages and 4500 malformed messages) was used for training and testing. They achieved 99.89% detection accuracy; however, they did not mention how they fine-tuned the SVM classifier.

6. Analysis of Surveyed Approaches

Analysis of the main characteristics of the surveyed approaches is presented in Table 2. We have analyzed the previous approaches by publication year, detection approach, detected attacks, detection time, and performance. The detection approach shown in these tables is the main algorithm(s) used to detect the attacks. In addition, different types of detected attacks (e.g., INVITE flooding and malformed message) are presented for each approach. Most of the surveyed approaches were tested against flooding attacks especially the INVITE flooding while a few numbers of these approaches were experienced against other DoS attacks such as malformed messages or DDoS attacks.

Since surveyed approaches are affected by different factors such as hardware configuration, we have presented detection time and performance as indicators to evaluate an approach's applicability in real VoIP networks. It has been found that more than half of the surveyed approaches did not measure the detection time. In addition, some of them reported a high detection time such as [30]. Moreover, they used different performance measures such as F1 score, accuracy, and detection probability which difficulties the comparison of surveyed approaches' performance.

It is worth mentioning that almost all the work surveyed uses a simulated dataset, excluding [46,49] where real datasets are used. In [23], the authors tried to mimic a real dataset by using a simulated dataset with one server and nine clients in different regions connected via the internet. The issue of using a dataset with a slight difference between normal and attack messages was tackled in [46].

Table 2. Analysis of the characteristics of surveyed approaches.

Reference	Year	Detection Approach	Detected Attacks	Detection Time	Performance
Finite State Machine Approaches					
[22]	2018	FSM and Fuzzy Logic	Flooding	-	Detection Probability 99.9%
[23]	2017	FSM and Whitelist	Flooding and DDoS	1.5 s	-
Rules Based Approaches					
[24]	2019	Rules Based SDP Parser	Malformed Message	17–60 ms	Accuracy: 100%
[25]	2018	Rules Based and FSM	INVITE Flooding	-	Accuracy: 100%
[26]	2016	Fuzzy logic and CUSUM	INVITE Flooding	Low-rate: 40.5 s High-rate: 5–24 s	Accuracy: 93.8% Accuracy: 100%

Table 2. *Cont.*

Reference	Year	Detection Approach	Detected Attacks	Detection Time	Performance
[27]	2016	Rules Based	INVITE, REGISTER, and BYE Flooding	High-rate: 500 ms	-
[30]	2018	Rules-based and Bloom Filter	Flooding	9 s	FP: 0.008–1.5% FN: 0.002–0.005%
			Fake Signaling	12 s	FP: 1.6–2% FN: 4.13–5%
[31]	2016	Statistics and Rules Based	Two new DDoS	-	-
Statistically Based Approaches					
[33]	2014	Sketch design and HD	Flooding and DDoS	-	Detection Probability 100%
[34]	2014	Sketch design and Entropy	INVITE, Combinational, and Distributed Flooding	-	Detection Probability 94.7–100%
[28]	2015	Rules Based and Hash Table	INVITE Flooding	-	-
[35]	2015	String comparison Chi-Squared Test	Malformed Message and Flooding	-	FP: 0% FN: 1.6–4.8%
[36]	2015	Entropy	INVITE flooding	1.8–16.8 ms	FP: 0.3–10.6% FN: 0.9–1.8%
[37]	2014	Tanimoto Distance and Trust Model	INVITE Flooding	-	Accuracy: 95%
[38]	2016	Poisson Distribution	Single and Multi Attribute Flooding	-	Accuracy: 100%
[39]	2015	Adaptive Thresholds		-	Detection Rate
			INVITE Flooding		95.95–98.05%
			SPAM		88.3–90%
[19]	2016	Event System and State Transition	Single and Multi Attribute Flooding	-	Accuracy: 100% Accuracy: 99%
[21]	2018	Change Point Model	DDoS flooding	0.76 ± 0.45 s	F1: 88%
[40]	2018	Bayesian Change Point Model	DDoS flooding	2 ms	Avg. F1: 95%
Machine Learning Approaches					
[42]	2015	SVM Classifier	REGISTER, RINGING and INVITE Flooding	100 ms - 2 s	Accuracy: 95–97%
[44]	2017	SVM Classifier	INVITE Flooding	2.057–2.384 s	Accuracy: 99.9% FP: 0%, FN: 0.27%
[45]	2015	SVM and Entropy	Flooding and Malformed Message	-	Detection Rate: 95%
[46]	2015	C5.0, SLIPPER, and SVM Classifiers	Malformed Message	0.2236 ms	Accuracy: 98.49–99.73%
[48]	2019	Linear SVM Classifier	Flooding and SPIT	0.7370 ms	F1: 100%
			Malformed Message	0.5702 ms	F1: 100%
[49]	2014	Naive Bayes and Decision Tree	Flooding DoS and DDoS	25.571 ms	TP: 92–100% FP: 0–0.8%
			SPIT	-	TP: 0–95.1% FP: 0–1%
[41]	2015	5 Different Classifiers	DoS	-	FP: 0–0.08% FN: 0–0.01%
			DDoS		FP: 0–5.2% FN: 0%
[50]	2016	SVM Classifier	DoS and DDoS Malformed Message	-	Accuracy: 99.89%

Table 3 highlight the strengths and weaknesses of the surveyed approaches. We considered static thresholds as a weakness because they do not consider SIP temporal characteristics. Moreover, they are not dynamically updated by attack behavior. In addition, any detection time exceeding one second was considered as a weakness because such approaches are not applicable in VoIP networks.

A few numbers of the surveyed approaches have implemented FSM while the larger portion of them depended on statistically based approaches. In addition, most of the rules-based and statistically based approaches used thresholds to fine-tune system performance. These thresholds may be calculated over a long period of SIP traffic as in [31] or consume system resources such as [19].

Table 3. Strengths and weaknesses of surveyed approaches.

Reference	Strengths	Weaknesses
Finite State Machine Approaches		
[22]	- CDR data usage. - Determination of attack severity (normal, alarm, or attack).	- Fine-tuning of the fuzzy system. - Selecting a proper time window.
[23]	- Consideration of attack intensity. - A whitelist algorithm that needs little computation resources. - Many attack scenarios are tested. - Attack sources are deployed on different sites.	- Usage of many dynamic thresholds. - Need for high detection time.
Rules Based Approaches		
[24]	Usage of the SDP part of the SIP message.	- The parser rules are dedicated to the SDP part of the SIP message only.
[25]	The detection approach is implemented at the data plane.	- Usage of static thresholds. - Experiments were conducted on a high number of packets only. - Implementation of the proposed approach over every switch on the network is not applicable. - Limited to unencrypted packets.
[26]	Detection of low-rate and high-rate flooding attacks.	- Static thresholds are utilized. - The used rules are dedicated to flooding attacks, so other attacks are not detected. - In the case of low-rate attack, it has low accuracy. - High detection time is needed.
[27]	Different attack rates are tested.	- Static thresholds are used. - Stealthy and DDoS attacks cannot be detected.
[30]	- Many types of attacks are tested. - High detection accuracy is achieved in terms of FP and FN.	- Static thresholds are utilized. - Storing session database and usage of six hash functions consumed memory and CPU resources - Need for high detection time.
[31]	- CPU load of SIP server is decreased under attack with 73.4%. - The detection of two new DDoS attack scenarios is tested.	- The system performance is not measured. - Calculating eight thresholds over one hour of traffic may consume memory and CPU resources.
Statistically Based Approaches		
[33]	- DDoS attacks are examined.	- Stealthy flooding attack is not detected.
[34]	- Many flooding attacks scenarios are tested.	- Low detection probability is established in case of combinational attack. - Inability to detect the stealthy attack. - Training and testing interval lengths are related to the network traffic. - The beginning of the detection process depends on network traffic-free from attacks.
[28]	Has not been noticed.	- Usage of a static threshold. - Storing an entry for every call may consume system memory. - SIP proxy server changes are required. - The system performance is not measured.
[35]	Malformed and flooding attacks are detected.	- Usage of many thresholds. - Calculating the Chi-square test consumes resources and time. - The proposed black-list stores the SIP address only.
[36]	- Usage of audit trails data. - Users' privacy-preserving is kept. - Offline and online executions are done.	- Many thresholds are used. - Offline detection is more robust than online. - Requiring at least one attack-free audit trail. - High detection time is needed.
[37]	- Low computing resources are required. - Handling suddenly or dynamic increase of legitimate traffic.	Choosing an appropriate testing window size to achieve high accuracy.

Table 3. *Cont.*

Reference	Strengths	Weaknesses
[38]	- Usage of continuous learning to update the normal traffic model. - Testing different rates of flooding attacks. - Utilizing 38 h dataset.	- Usage of static thresholds. - The training period is fixed (10 min). - The tested attacks are generated using a custom tool implemented by the authors.
[39]	Simple implementation.	- Adaptive thresholds are updated at fixed times - Having a low detection accuracy, especially in case of low-rate flooding and SPAM attack. - The multi-attribute attack is not detected.
[19]	Detecting many types of attacks.	- Low-rate attacks are not tested. - Ten static thresholds should be calculated during the training.
[21]	- In addition to the detection of the attack messages, the attacker is also identified. - Making use only of the type and intensity of the VoIP traffic through an unsupervised approach. - Calculating four parameters only to adjust the model.	- Low detection accuracy is achieved. - System performance is highly dependent on the observation interval. - The best F1 score is achieved with 10 s sampling interval which is considered a long time to raise attack alarm. - System parameters should be updated to account for the VoIP traffic intensity.
[40]	- The used techniques can be customized according to server parameters. - Features are extracted from SIP messages and server logs. - Utilizing different features allows capturing the diversity of SIP messages. - 40 different DDoS attacks are tested.	- Memory and CPU resources are consumed due to extracting 41 features and calculating ten model parameters. - High detection time is needed.
Machine Learning Approaches		
[42]	- Statistical features are used to capture the diversity of SIP messages. - Features are calculated over a window of SIP messages capturing the correlation between them. - Different attacks are tested using two datasets.	- Calculating 18 features over a window of SIP messages takes a considerable amount of processing time. - Some of the features are redundant (i.e., 200 OK messages are a part of response messages). - Giving a high positive false rate.
[44]	- Usage of a small number of non-redundant features. - Low and high-rate flooding attacks are detected. - High detection accuracy with zero FP.	- Waiting for the fullness of the packet buffer may delay the raise of attack alarm. - High detection time is needed.
[45]	Network traffic is classified into VoIP and non-VoIP.	- Usage of static thresholds.
[46]	- Using the *n*-gram technique, a generic feature extraction technique, not dedicated to a specific attack. - Using dataset with a slight difference between normal and attack messages. - Low detection time is accomplished. - Three classifiers are used to achieve high detection accuracy. - Attacks of encrypted traffic are detected.	- Feature extraction using the *n*-gram technique takes a considerable amount of processing time. - Calculating *n*-grams message by message does not capture the correlation between successive messages. - The complexity of implementation. - The normal traffic gets serviced twice; by the proposed approach and the SIP server.
[48]	- Using the *n*-gram technique, a generic feature extraction technique, not dedicated to a specific attack. - Low detection time is established. - Two different datasets are used.	- Feature extraction using the *n*-gram technique takes a considerable amount of processing time. - Calculating *n*-grams message by message does not capture the correlation between successive messages. - Low-rate and DDoS attacks are not tested.
[49]	- Usage of purely packet-based instead of flow-based. - A small number of features are calculated. - A real dataset from a VoIP service provider is used. - Six attack scenarios are tested.	- Calculation of the features every 40 packets may delay the raise of attack alarm. - Different features for every attack are calculated. - Low-rate attacks are detected with low accuracy.
[41]	- Different classifiers are utilized over many attack scenarios. - Detection of DoS and DDoS attacks.	- Usage of a 1000 SIP message window may delay the raise of attack alarm. - Low-rate attacks are identified with low accuracy.
[50]	- The kernel tree is used to reduce parsing time. - Testing of different types of malformed messages. - Detection of DoS and DDoS attacks.	- Usage of a small dataset containing 5000 SIP messages only. - Details of DDoS scenarios and classifier fine-tuning are not listed.

Most of the surveyed approaches have classified the SIP messages into normal or malicious while others have determined the attack severity (e.g., [22]) or the intensity of the attacks (e.g., [49]). In addition, only the proposed approach in [21] has identified the attackers from legitimate users.

It is noted that the surveyed approaches vary in attack testing. Some of them developed different attack scenarios and different attack rates (i.e., low and high) while others were not. Considering implementation, some of the proposed approaches require deployment over every switch on the network [25] or changing the SIP proxy server [28]. This in turn produces considerable difficulty.

Feature extraction is an important process in ML approaches. The majority of the surveyed ML approaches extracted features from SIP headers and haven't used other resources such as server log files [40] or CDR [22]. In addition, some of these approaches such as [42,49] have calculated features over a group of SIP messages to capture the correlation between messages, while others such as [46,48] have extracted features over one by one SIP messages to achieve faster detection time. For those that used a group of SIP messages, they should choose an appropriate number of SIP messages to be processed (i.e., buffer size) to balance between achieving high performance and fast detection time.

Using multiple classifiers together was introduced in [46] while other ML proposed approaches used only one classifier, which usually was the SVM classifier. Moreover, the usage of continuous learning to update the normal traffic model was implemented in [38] to keep the system updated with the expected change in normal traffic behavior.

7. Challenges and Future Directions

From the assessment of the before mentioned approaches, several challenges can be distinguished. In this section, we will be exposed to several of them. Dependent on these obstacles, guidelines for future research directions shall be provided. One of the major challenges in DoS or DDoS detection is that proposed approaches can detect only high-rate flooding attacks. On the other hand, they show poor performance against low-rate flooding attacks. Furthermore, a considerable percentage of the suggested approaches are incapable of facing malformed message attacks.

Additionally, many proposed approaches are designed for specific working conditions. We have noticed also that some approaches do not dynamically adapt to detect unknown attacks which constitute a notable obstacle against their usage. Most approaches relying on SIP messages for features extraction suffer from a significant drawback. In fact, they depend on SIP headers only and don't make use of other valuable resources such as CDR or SIP server log files that contain useful information (e.g., CPU and memory usage). In addition, some approaches involve the computation of a large number of features that requires a significant amount of memory and result in increased processing overhead.

Moreover, some of the proposed approaches did not take into consideration the complexity and diversity of DoS and DDoS attacks resulting in the negligence of false alarms leading to bad consequences. Finally, we believe that although machine learning techniques are promising, yet there is a desperate need for a publicly available SIP dataset to be used as a benchmark for further research work. Additionally, a unified performance measure (e.g., F1 score) is needed to evaluate these techniques.

The previously mentioned challenges inspire the following research directions. First of all, since new versions of DDoS attacks are emerging, hence there is a need to design techniques utilizing dynamic detection adaptable for these new versions. Moreover, efficient detection techniques are required since most available techniques emphasize the detection results; therefore, they usually employ complex models and extensive data preprocessing methods, leading to low efficiency. To be noted that real-time detection techniques constitute a booming research direction especially on emerging network environments such as the Internet of Things (IoT) and mission-critical cloud networks. In these networks, lightweight techniques are needed which combine effect and efficiency.

Lastly, machine learning approaches are promising in their results and will open new research paradigms especially deep learning techniques. Unfortunately, the lack of available datasets inspires the need for updated datasets reflecting new attacks. However, constructing new datasets depends

on expert knowledge for labeling which is costly and time-consuming. Moreover, the available datasets should be characteristic, balanced, and have less redundancy and noise. Organized datasets construction and incremental learning may be solutions for this problem.

8. Conclusions

VoIP systems worldwide have recently been taking over traditional solutions because of their low cost and high quality of service for voice and multimedia communications. SIP, the dominant protocol for signaling operations in VoIP, is vulnerable to many types of attacks; DoS and DDoS are serious attacks since they prevent legitimate users from reaching VoIP services. In this survey, we categorized recent DoS and DDoS detection approaches into FSM approaches, rules-based approaches, statistically based approaches, and machine learning approaches. Then, we analyzed them with respect to many factors such as detected attacks and performance. Additionally, we highlighted the strengths and weaknesses of the different approaches. By doing so, the survey determined the existing challenges against efficient detection of DoS and DDoS attacks. Furthermore, it outlined future research directions for improving attack detection performance.

Author Contributions: Conceptualization, W.N., W.S.E., and T.A.; formal analysis, W.N.; investigation, W.N.; writing, original draft preparation, W.N.; writing, review and editing, W.N., W.S.E., T.A., and H.D.; visualization, W.N.; supervision, W.S.E. and T.A.; funding acquisition, W.S.E. and H.D. All authors read and agreed to the published version of the manuscript.

Funding: The authors extend their appreciation to the Deanship of Scientific Research at King Saud University for funding this work through Research Group No. (RG-1439–039).

Acknowledgments: The authors thank the Deanship of Scientific Research and RSSU at King Saud University for their technical support.

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

References

1. Inc, C. Cisco Visual Networking Index: Forecast and Trends, 2017–2022 White Paper. Available online: http://goo.gl/X3efVF (accessed on 7 June 2020).
2. Nettitude. VoIP Attacks on the Rise. 2015. Available online: https://www.nettitude.com/uk/ (accessed on 7 June 2020).
3. Alo, U.; Firday, N.H. Voice over internet protocol (VOIP): Overview, direction and challenges. *J. Inf. Eng. Appl.* **2013**, *3*, 18–28.
4. Jacobson, V.; Frederick, R.; Casner, S.; Schulzrinne, H. RTP: A transport protocol for real-time applications. 2003. Available online: https://tools.ietf.org/html/rfc3550 (accessed on 15 June 2020).
5. Rosenberg, J. SIP: Session Initiation Protocol. 2002. Available online: https://tools.ietf.org/html/rfc3261 (accessed on 15 June 2020).
6. Keromytis, A.D. A comprehensive survey of voice over IP security research. *IEEE Commun. Surv. Tutor.* **2011**, *14*, 514–537.
7. Cooney, M. IBM Warns of Rising VoIP Cyber-Attacks, Technical Report. 2016. Available online: https://www.networkworld.com/article/3146095/ibm-warns-of-rising-voip-cyber-attacks.html (accessed on 7 June 2020).
8. Raza, N.; Rashid, I.; Awan, F.A. Security and management framework for an organization operating in cloud environment. *Ann. Telecommun.* **2017**, *72*, 325–333.
9. Arshad, J.; Azad, M.A.; Amad, R.; Salah, K.; Alazab, M.; Iqbal, R. A Review of Performance, Energy and Privacy of Intrusion Detection Systems for IoT. *Electronics* **2020**, *9*, 629.
10. Rathore, S.; Sharma, P.K.; Loia, V.; Jeong, Y.S.; Park, J.H. Social network security: Issues, challenges, threats, and solutions. *Inf. Sci.* **2017**, *421*, 43–69.
11. Azad, M.A.; Morla, R.; Salah, K. Systems and methods for SPIT detection in VoIP: Survey and future directions. *Comput. Secur.* **2018**, *77*, 1–20.
12. Naeem, M.M.; Hussain, I.; Missen, M.M.S. A survey on registration hijacking attack consequences and protection for Session Initiation Protocol (SIP). *Comput. Netw.* **2020**, *175*, 107250.

13. Azrour, M.; Ouanan, M.; Farhaoui, Y. Survey of SIP Malformed Messages Detection. *Indones. J. Electr. Eng. Comput. Sci.* **2017**, *7*, 457–465.
14. 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.
15. Ganesh, M.L.; Pravinkumar, D.; VinodiniM, S.; AbhejitS, K. Survey of Dos Attacks, Detections &Prevention Frameworks for SIP Proxy Server. *Int. J. Innov. Res. Sci. Eng. Technol.* **2014**, *3*, 904–910.
16. Armoogum, S.; Mohamudally, N. Survey of practical security frameworks for defending SIP based VoIP systems against DoS/DDoS attacks. In Proceedings of the 2014 IST-Africa Conference Proceedings, Le Meridien Ile Maurice, Mauritius, 7–9 May 2014; pp. 1–11.
17. Perkins, C. SDP: Session description protocol. *Internet RFC* **2006**, *4566*, 1–49.
18. Zar, J. VoIP security and privacy threat taxonomy. 2005. Available online: https://www.voipsa.org/Activities/VOIPSA_Threat_Taxonomy_0.1.pdf (accessed on 7 June 2020).
19. Golait, D.; Hubballi, N. Detecting anomalous behavior in VoIP systems: A discrete event system modeling. *IEEE Trans. Inf. Forensics Secur.* **2016**, *12*, 730–745.
20. Ferdous, R. SIP-Msg-Gen : SIP Message Generator. 2012. Available online: https://github.com/rferdous/SIP-Msg-Gen (accessed on 15 June 2020).
21. Semerci, M.; Cemgil, A.T.; Sankur, B. An intelligent cyber security system against DDoS attacks in SIP networks. *Comput. Netw.* **2018**, *136*, 137–154.
22. Hosseinpour, M.; Yaghmaee, M.H.; Hosseini Seno, S.A.; Khosravi Roshkhari, H.; Asadi, M. Anomaly-based DoS detection and prevention in SIP networks by modeling SIP normal traffic. *Int. J. Commun. Syst.* **2018**, *31*, e3825.
23. 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.
24. Tsiatsikas, Z.; Kambourakis, G.; Geneiatakis, D.; Wang, H. The Devil is in the Detail: SDP-Driven Malformed Message Attacks and Mitigation in SIP Ecosystems. *IEEE Access* **2019**, *7*, 2401–2417.
25. Febro, A.; Xiao, H.; Spring, J. Telephony Denial of Service defense at data plane (TDoSD@ DP). In Proceedings of the NOMS 2018—2018 IEEE/IFIP Network Operations and Management Symposium, Taipei, Taiwan, 23–27 April 2018; pp. 1–6.
26. Sun, Q.; Wang, S.; Lu, N.; Wong, K.S.; Kim, M.H. SFADS: A SIP Flooding Attack Detection Scheme with the Internal and External Detection Features in IMS Networks. *J. Internet Technol.* **2016**, *17*, 1327–1338.
27. Cadet, F.; Fokum, D.T. Coping with denial-of-service attacks on the IP telephony system. In Proceedings of the SoutheastCon 2016, Norfolk, VA, USA, 30 March–3 April 2016; pp. 1–7.
28. Bansal, A.; Pais, A.R. Mitigation of Flooding Based Denial of Service Attack against Session Initiation Protocol Based VoIP System. In Proceedings of the 2015 IEEE International Conference on Computational Intelligence & Communication Technology, Ghaziabad, India, 13–14 February 2015; pp. 391–396.
29. Roesch, M. Snort: Lightweight intrusion detection for networks. In Proceedings of the LISA 99: 13th Systems Administration ConferenceSeattle, Washington, DC, USA, 7–12 November 1999; Volume 99, pp. 229–238.
30. Ganesan, V.; Msk, M. A scalable detection and prevention scheme for voice over internet protocol (VoIP) signaling attacks using handler with Bloom filter. *Int. J. Netw. Manag.* **2018**, *28*, e1995.
31. 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.
32. 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.
33. 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.
34. Zargar, R.H.M.; Moghaddam, M.H.Y. An entropy-based VoIP flooding attacks detection and prevention system. In Proceedings of the 2014 4th International Conference on Computer and Knowledge Engineering (ICCKE), Mashhad, Iran, 29–30 October 2014; pp. 691–696.
35. Su, M.Y.; Tsai, C.H. An approach to resisting malformed and flooding attacks on SIP servers. *J. Netw.* **2015**, *10*, 77.
36. Tsiatsikas, Z.; Geneiatakis, D.; Kambourakis, G.; Keromytis, A.D. An efficient and easily deployable method for dealing with DoS in SIP services. *Comput. Commun.* **2015**, *57*, 50–63.

37. Chaisamran, N.; Okuda, T.; Kadobayashi, Y.; Yamaguchi, S. SIP Flooding Attack Detection Using a Trust Model and Statistical Algorithms. *J. Inf. Process.* **2014**, *22*, 118–129.
38. Golait, D.; Hubballi, N. Voipfd: Voice over ip flooding detection. In Proceedings of the 2016 Twenty Second National Conference on Communication (NCC), Guwahati, India, 4–6 March 2016; pp. 1–6.
39. Lee, J.; Cho, K.; Lee, C.; Kim, S. VoIP-aware network attack detection based on statistics and behavior of SIP traffic. *Peer Peer Netw. Appl.* **2015**, *8*, 872–880.
40. 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.
41. Tsiatsikas, Z.; Fakis, A.; Papamartzivanos, D.; Geneiatakis, D.; Kambourakis, G.; Kolias, C. Battling against DDoS in SIP: Is Machine Learning-based detection an effective weapon? In Proceedings of the 2015 12th International Joint Conference on e-Business and Telecommunications (ICETE), Colmar, France, 20–22 July 2015; Volume 4, pp. 301–308.
42. Asgharian, H.; Akbari, A.; Raahemi, B. Feature engineering for detection of Denial of Service attacks in session initiation protocol. *Secur. Commun. Netw.* **2015**, *8*, 1587–1601.
43. Nassar, M.; State, R.; Festor, O. Labeled VoIP data-set for intrusion detection evaluation. In *Meeting of the European Network of Universities and Companies in Information and Communication Engineering*; Springer: Berlin/Heidelberg, Germany, 2010; pp. 97–106.
44. Pougajendy, J.; Parthiban, A.R.K. Detection of SIP Based Denial of Service Attack Using Dual Cost Formulation of Support Vector Machine. *Comput. J.* **2017**, *60*, 1770–1784.
45. Vennila, G.; Manikandan, M.; Aswathi, S. Detection of SIP signaling attacks using two-tier fine grained model for VoIP. In Proceedings of the TENCON 2015-2015 IEEE Region 10 Conference, Macao, China, 1–4 November 2015; pp. 1–7.
46. Marchal, S.; Mehta, A.; Gurbani, V.K.; State, R.; Ho, T.K.; Sancier-Barbosa, F. Mitigating Mimicry Attacks Against the Session Initiation Protocol. *IEEE Trans. Netw. Serv. Manag.* **2015**, *12*, 467–482.
47. Hall, M.; Frank, E.; Holmes, G.; Pfahringer, B.; Reutemann, P.; Witten, I.H. The WEKA data mining software: an update. *ACM SIGKDD Explor. Newsl.* **2009**, *11*, 10–18.
48. Nazih, W.; Hifny, Y.; Elkilani, W.; Abdelkader, T.; Faheem, H. Efficient Detection of Attacks in SIP Based VoIP Networks using Linear l1-SVM Classifier. *Int. J. Comput. Commun. Control.* **2019**, *14*, 518–529.
49. Akbar, M.A.; Farooq, M. Securing SIP-based VoIP infrastructure against flooding attacks and Spam Over IP Telephony. *Knowl. Inf. Syst.* **2014**, *38*, 491–510.
50. Akbar, A.; Basha, S.M.; Sattar, S.A.; Raziuddin, S. An intelligent SIP message parser for detecting and mitigating DDoS attacks. *Int. J. Innov. Eng. Technol.* **2016**, *7*, 1–7.