Intrusion Detection and Prevention System for Secure Multimedia sharing in Future Internet

HUMAIRA ASHRAF , ATA ULLAH , SHIREEN TAHIRA , Noor Jhanjhi *

Posted Date: 18 January 2024

doi: 10.20944/preprints202401.1313.v1

Keywords: IDS; IMS; IoT; LTE; Multi-media Sharing

Article

Intrusion Detection and Prevention System for Secure Multimedia sharing in Future Internet

Humaira Ashraf [1], Ata Ullah [2], Shireen Tahira [1], Nz Jhanjhi [3,*]

[1] Department of Computer Science and Software Engineering, International Islamic University, Islamabad, Pakistan; humaira.ashraf@iiu.edu.pk; shireentahira381@gmail.com

[2] Department of Computer Science. National University of Modern Languages, Islamabad, Pakistan; aullah@numl.edu.pk

[3] School of Computer Science and Engineering, SCE, Taylor's University, Malaysia; noorzaman.jhanjhi@taylors.edu.my

* Correspondence: NZ Jhanjhi; noorzaman.jhanjhi@taylors.edu.my

Abstract: IP Multimedia Subsystem (IMS) supports high-speed transmission of multi-media like data, audio, and video between mobiles and other wireless devices. IMS is the most suitable for multimedia communication across multiple networks using the Internet of Things (IoT) and cloud computing. IoT-IMS can efficiently manage the huge amount of data generated by smart devices for audio-video during live streaming applications. During these services, the main problem is that an intruder can launch a Session Initialization Protocol (SIP) messages flooding attack on IMS that does not have the functionality to prevent itself from these types of attacks. In this paper, an intrusion detecting and preventing system (IDPS) is proposed that effectively detects the register flooding and spoofing attacks using SIP messages. We proposed a watermark embedding algorithm on the user side and an extraction algorithm on receiving side. A test-bed is set up for IMS where we have considered four different scenarios to evaluate the IDPS approach as compared to counterparts. Results illustrate the dominance of our scheme in terms of response time, register flooding attack detection ratios, CPU load utilization, fault detection ratio, and memory utilization. The fault detection ratio averagely 98.18.

Keywords: IDS; IMS; IoT; LTE; multi-media sharing

1. Introduction

Due to the huge number of ubiquitous devices like laptops smartphones, etc., IoT-assisted multimedia sharing has gained the growing interest of researchers. Such networks employ IMS which is an architectural framework that provides multimedia services to the users of mobile devices. IoT-IMS can manage the huge traffic generated for sharing multimedia data in streaming applications. IMS architecture is divided into three layers i.e. control layer, service layer, and transport layers which are illustrated in Figure 1. The control layer makes the policy decisions also provide session management, the service layer comprises hosts and application servers, the transport layer connects the access layers and IP networks. The Transport layer It is an beginning side of the point from claiming IMS organize with range during IMS core, the place it allots a ip address, default gateways and Enlistment gadgets on clients from upper layer. The Control layer The center capacity of this layer is on furnish session control with users; they would bring session control capacity (CSCF). There would three sorts for CSCF functions, Proxy-CSCF (P-CSCF), Interrogating-CSCF (I-CSCF), and Serving-CSCF (S-CSCF). CSCF's need aid session start protocol (SIP) servers. The Content sharing at IMS, security, and privacy is a concern [1]. The There are three sorts from claiming administration works given Toward this layer. They are; media asset capacity controller (MRFC), media asset capacity processor (MRFP), and requisition server. MRFC Also MRFP they both give administrations similar to publication Also conferencing for those clients. MRFC handle taste correspondence with the S-CSCF.A peer-to-peer architecture also supports a core network for providing more secure and novel services. It analyzes voice-call traffic data to analyze the performance of novel architecture [2]. A dual server-based architecture also achieves better attacks detection for INVITE flooding using the

 doi:10.20944/preprints202401.1313.v1

main server and cooperative sever. It also applies three thresholds to generate alarms as per attack detection [3–5]. An intrusion detection system (IDS) is mandatory to secure services and signaling as well. Distributed nature of attacks is quite possible due to bot-net attacks where multiple machines at a different location launch a distributed denial-of-service attack. In IDS, signature-based approaches use known patterns whereas anomaly detection works for unknown patterns [6]. The IDS proposed in [7] operates hierarchically by using control systems. The local information is obtained and then the results are transferred to the upper level after review [8].

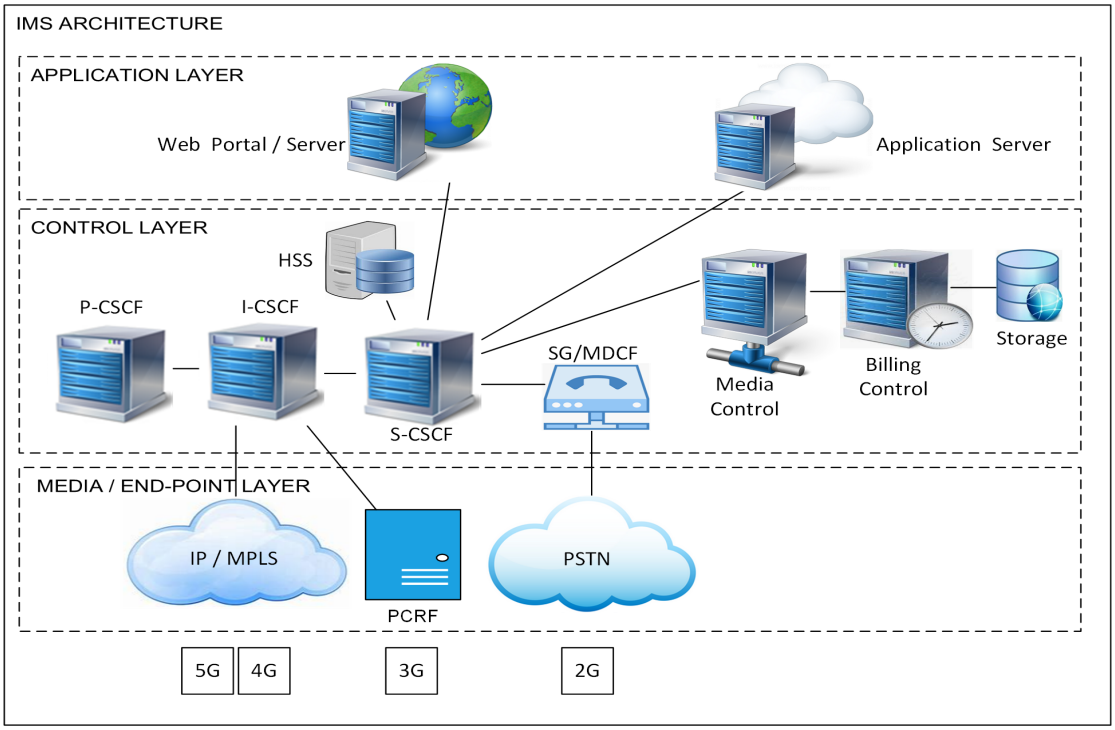


Figure 1. The architecture of IP Multimedia Subsystem.

The IMS is effected by registeration flooding attacks and spoofing attacks which increases the need of IDS, which identifies the threats after collecting information throughout the network either from a single host or a single network interface or from multiple locations. IDS should be able to track and avoid attacks and should be sensitive to a fault. A two-stage Next Generation Networks (NGN) intrusion detection model is capable of handling the threats. During data exchange for multimedia applications, intermediaries like recorders are needed at the media path. An end-to-middle-to-end solution can provide secure communication [8,9]. In a similar vein, an adaptive data collection mechanism uses heuristic algorithms along with synthetic attack recognition. It helps to secure the data exchange through intermediaries as well by adapting the change in attack patterns [10]. It is applicable in Voice Over IP (VoIP) infrastructures of IMS where SIP protocol is responsible for session setup and session handling. The free syntactic standards and text-based message structure provide a the lightweight, adaptable convention that achieves high QoS with low response times [11]. A verification component such as AKA especially with IPSec [12] cannot hold hazards starting from Internal Attackers (IAs) digging down IPSec. An attacker may post an ARP attack with the end goal of gathering the Authentication Vectors (AV) from a handshake that may break the validation framework or capture correspondence. A protection framework can help to detect/avoid threats from outside attackers. However, after authentication insider, malevolent clients may start attacks by pretending to be a legitimate users. Public key infrastructure is used for authentication but no self-healing keys are provided.

This paper presents an IDPS (Intrusion Detection and Prevention System) for the detection and prevention of flooding and spoofing attacks on the IMS. An IDS has two subsystems, one is

 doi:10.20944/preprints202401.1313.v1

responsible for the detection and prevention of spoofing and the other is responsible for detection and prevention of flooding.

For the detection of spoofing attacks, a zero watermarking scheme is proposed. The delay is minimized by avoiding the comparisons with previously stored IP addresses. This comparison is avoided because the watermark is not embedded in the IP address rather it is generated from it. The technique of watermarking has two levels: (1) the embedding algorithm (2) the extraction algorithm. Watermark embedding is done to prove the ownership of the original author and the extraction is done by Key Management Center (KMC) later. The KMC is a trusted authority in this algorithm where the original owner has to register its watermark with.

The paper is structured as: Section 2 explores literature review and Section 4 elaborates the proposed IDPS along with a description for embedding and extraction algorithms. Section 5 shows the results and analysis. This work is concluded in Section 6.

Contributions

The contribution of this research is mentioned below:

1. Ayanlizing the need for Intrusion Detection Systems (IDS) for flooding and spoofing attacks in the IMS environment
2. This presents an IDPS (Intrusion Detection and Prevention System) for the detection and prevention of flooding and spoofing attacks on the IMS
3. An two subsystem based IDS proposed has one subsystem which is responsible for the detection and prevention of spoofing and the other is responsible for detection and prevention of flooding.
4. For the detection of spoofing attacks, a zero watermarking scheme is proposed.
5. The delay is minimized by avoiding the comparisons with previously stored IP addresses. This comparison is avoided because the watermark is not embedded in the IP address rather it is generated from it.

2. Literature Review

We have evaluated the intrusion detection schemes and discussed the impact of different types of attacks during the communication between users and servers. It also explores the attack mitigation schemes. A self-enforcing protocol is proposed for authentication in next-generation networks using SIP is mentioned in [13]. The key issue is that data from VoIP / IMS communication can be manipulated at layers 2, 3, or 5. The key attack classes for the application layer are: manipulation of SIP signaling, masquerade, Man in the Middle (MitM), and replay attacks. In signaling attacks, the attacker exploits SIP protocol requests so that DoS takes place on the server or a specific user. The CANCEL request is responsible to revoke a multimedia session whereas the BYE request terminates the multimedia sessions affecting the quality of service [14]. The headers of such that include From and Call-id are spoofed by an attacker to terminate the session illegally. Such attacks can be launched over the security tunnels by an IA specifically if the parser's implementation is weak. Moreover, registration procedure data exchange through intermediaries as well by adapting the change in attack patterns [10] is time-consuming and complex. We note that if the user sends only two register requests, this results in 20 messages inside the network. Unless any spoofed IP lunches flood attack, otherwise IMS ecosystem will be heavily affected. If a flooding attack is launched, the request will be rejected every time due to unregistered identity messages that generate tremendous network traffic.

The primary requirement for a dependable network is to provide security to critical information being exchanged using Voice Over Lightweight evolution (VOLTE) [15]. Moreover, continuous and congestion-free service is also the key requirement to fulfill customer satisfaction as per demanded QoS. SIP is the major protocol used in all VoIP architectures. Quality evaluation methods [16] and SIP-based authentication and key agreement schemes are explored in terms of securing the communication sessions [17]. Security weaknesses of SIP are explored where an attacker may pick up the IP address of an authentic client of VOLTE. It utilizes an initiating request of the client and an attack is launched wherein the attacker the gained IP of the client [18].

 doi:10.20944/preprints202401.1313.v1

Service denial attacks can be propelled by using an UPDATE request or a re-INVITE request. Particularly, the invader may hijack a multimedia session as mentioned in [19,20]. Malicious clients are set as correspondent among the client and the server that is a Man in Middle (MitM) attack [21]. In this kind of attack, the aggressor sidesteps both honesty and legitimacy, security prerequisites. It is capable to imitate clients or system components for unapproved access to the administrations, capturing the channels, or even denial of administration. These attacks can be propelled by using either Address Resolution Protocol(ARP) harming [22] (in layer 2) or Domain Name System (DNS) harming (in layer 5) [23] strategies. Assailant changes the IP-MAC or the area IP affiliations correspondingly keeping in mind the end goal to divert the traffic through him (going about as portal) and accumulates correspondence channels information. Truth be told, in VoIP/IMS foundations, an ARP or DNS balancing attack takes after a SIP-based attack where the messages are controlled, forcing further harm to the framework. The aggressor may parody the terminated header of an enlistment demand to zero creating quick deregistration of the casualty. Another attack can be propelled after an effective MitM by downsizing the security level of the up-and-coming session. Amid session foundation handshake, the halfway controls the header that incorporates accessible security suites and expels more grounded ones [24]. In [22], the attacker places itself between the proxy and (or the P-CSCF in IMS environments) and the user, masked from both of them. It soon gets access to AVs to get himself easily authenticated. This attack is based on SIP Digest authentication. In [21], authenticated spoofed requests and response messages are detected. Intruder acquires the user authentication vector to impersonate as a legitimate user to gain access to services. Resisting Malformed and Flooding Attacks [25] identify malformed messages to track distorted SIP messages for analyzing flooding attacks. The Chisquare check is carried out to find out whether the SIP server is getting attacks such as death, cancel, and flooding or not. Relative association of response massages is evaluated during the establishment of connection by using SIP. It adds the users to the blacklist to block the and flooding attacks. It reduces the flooding attacks on SIP through the request review scheme [26]. It does not change the layout of massage and avoids false registration, termination, and distorted message attacks. In [27] two key strategies are introduced, including IP tables and failure detection, to prevent the depletion of SIP resources in the form of Distributed Denial of Service (DDoS) attacks at a low rate. The IP tables dependent admission control method is used to secure the servers from unforeseen flooding attacks. In [24], the strategy reduces flooding attacks on SIP by way of call evaluation.

The multi-layer architecture for SIP-based VoIP systems is secured by providing security, confidentiality, integrity, and availability. SIP servers are protected against invalid registration requests and DDoS attacks. It updates user information in the database. The scheme also considers adding users to the blacklist that causes flooding attacks [28]. The model is dependent on the simultaneous shadowing of the attack rate, serving the proportion of requests and the average response time. It can reliably identify different types of flooding attacks and lower the false positive rate. It nullifies being influenced with the selection of threshold issue by either the masking of the attack, variation of the attack and negative shift and variation [29].

The instinctual detection of attacks by VoIP over distributed networks [30] offers an analysis of data collected with a multilayer network of preceptors trained in many attacks. Preprocessing and authenticating the attack data is used for the self-organizing graph. Data malicious actions are detected through the identification nodes of the network that include the honeypot framework and the traffic monitoring scheme. This automated categorization with a low true positive server rate condenses the cost of attack identification [30]. The majority of VoIP protocols are vulnerable to flooding attacks which compromise the services. A rapid and general framework for detecting fraud in real-time is needed [31]. VFDS is an online anomaly detection system that focuses primarily on INVITE, SYN, and RTP floods. The various features of the protocols shall be evaluated and the inherent relation between these characteristics identified by network traffic. The framework uses the distance between Hellinger and calculates variation between distributions of probability of data obtained from the network. Experimental findings show that vFDS is high in lower time detection accuracy [32]. An M/M/1/(K/2) model of scientific analysis analyzes and defends DEATH flood attack INVITE on SIP. The queue theory assimilates the benefits of existing protection mechanisms [8]. A SIP-based white list approach is about keeping the details about SIP users up to date. It retains the fields: User ID, last timestamp for registration, IP address, and registration termination date. This technique is not successful at handling botnet attacks with accepted credentials from compromised hosts. Its output can be improved by combining it with other mechanisms in the blacklist such as SIP Express Router (SER) or PIKE [33]. An automated analyzer is used to observe SIP messages and delete

 doi:10.20944/preprints202401.1313.v1

filtering rules, and a filter is used to prevent malicious massages. This tackles flooding attacks of SIP messages by reducing the rate of false-positive and false-negative [34].

In [35], the stream-based analysis approach detects hybrid flooding on SIP, introducing a multi-sample sliding window for mining statistical knowledge using a cumulative sum algorithm (CUSUM). The strategy is checked on low-intensity threats and high-intensity flooding. The suggested technique provides high precision, low false positives, and low power consumption for flood attack detection. Wavelet testing has been studied for stealthy flood detection that separates the variance generated by attacks from the original data. To achieve this it utilizes distorted coefficients from the original data. Sketch data structure is joined with the Hellinger distance to create a more robust and effective scheme. The author applies the Hellinger distance algorithm to the sketch data structure in [36] to define the difference between previous and present distributions of SIP request messages. Ehlert et al. combat flooding by offering a two layers' security policy where the first layer of a bastion host is used against the attacks of the network layer i.e. SIP Flooding and TCP SYN. SIP proxy with protection module is enhanced for offering advanced SIP security features. This is not an effective overhead and only works on proxy servers. It only guards DoS against SIP [37].

The machine learning algorithms, including CUSUM, Predictive threshold, and Hellinger distance are correlated and analyzed on the grounds of detection accuracy to identify flooding on various nasty traffic data set. Hellinger Range has a higher accuracy Trust recognition model based on a confidence value determined by the contact operation between the root (caller) and the recipient (callee). As per the provided formula, the allowed user's trust value must be higher than the intruder which is determined by the length and direction of the call among users. The trust-based model is united with CUSUM, Tanimoto Distance, and Hellinger Distance to assess the expected rate of false-positive and accuracy by applying it on mixed attack traffic [38]. Authors in [39] implemented VoIP Defender to track SIP traffic to prevent DDoS attacks. The architecture in question consists of a variety of assimilated techniques of detection and some techniques of attack reduction and prevention. In [40], shoket explored data sharing mechanism protection by using packet-level restriction to minimize DDoS attacks. Similarly, in [41] a vulnerability assessment system is proposed for the SIP susceptibilities through penetration testing and the generation of non-destructive SIP attacks. In [42], it describes the Multiple Classifier System's effectiveness toward mimicry attacks. It uses minimum detection measure (MDM) which is an Oracle-based fitness feature that limits system classifier maximum taxonomy efficiency. SIP anomaly detection schemes [43] use the datasets with variations to discover the anomaly. Regular packets are compared to anomalous packets are used to do so. It can detect anomalies by using trickier datasets by a feature reduction scheme. In [44] made clear the risk of multiple classifiers resisting SIP attacks based on the parser. Multiple classifier-based self-learning methods to detect the abnormally-shaped self-similar SIP massages. Similarly, the researcher in [45] discussed the reasons due to which the Euclidean distance-based classifiers were unable to achieve reliable results for malformed packets which differ slightly from normal packets. In [46], and SMS malformed message detection system is presented which captures syntactic features of smartphone SMS messages. In [47],the end-user keeps track of each arriving request's time and IP address. It updates the REGISTER request header by incrementing a new number. This holds the maximum number of users or the call value.

Nikos had expected an IMS and VoIP (IDSIVS) IDS. It included two modules namely the anti-spoofing module, and the entry request module. Requests are submitted with genuinely constructive and false-negative malicious requests mixed [48]. SSI was introduced in [49] that protects the SIP from flooding attacks. This senses the INVITE flood dynamically and compares it to a robust SIP system in real-time temporal characteristics. This system will which the detection time but is not capable of managing false alarms. Framework for intrusion detection and prevention i.e. DS-IDPS [5] is a dual server system. It provides defense against INVITE flooding attacks and spoofing. In [50], a novel IDS is proposed for the internet of medical things that are based on machine learning (ML) algorithms to distinguish between attack traffic and legitimate traffic. ML algorithm uses network and biometric parameters as features. Artificial intelligence algorithm is applied in the scheme proposed in [51]. It introduced an Anomaly Behavior Analysis Methodology based on Artificial Neural Networks that can be used to implement an adaptive IDS capable of detecting when a Fog node has been compromised and taking the necessary steps to restore communication availability. A lot of research is being carried out in the field of IoT regarding IDS. IoT and 5G are two technologies that will improve the user experience while also introducing new security risks such as DDoS and DoS. In [52] a scheme is proposed that tried to alleviate some of these issues by building an IDS and employing network slicing to locate and isolate the compromised resources. Expanding upon the

 doi:10.20944/preprints202401.1313.v1

groundwork established in prior research [53–62], this study explores the imperative domain of safeguarding multimedia sharing within the Future Internet.

3. Proposed Solution

The Intrusion Detection and Prevention System (IDPS) can detect spoofing and flooding attacks on the IMS network. It proposes two modules out of which one module utilizes zero watermarking for the detection of spoofing. The second module presents the identification and prevention of registered flooding. It uses anomaly detection and rule-based detection. The two key components of the network for IP spoofing and flooding are shown in Figure 2.

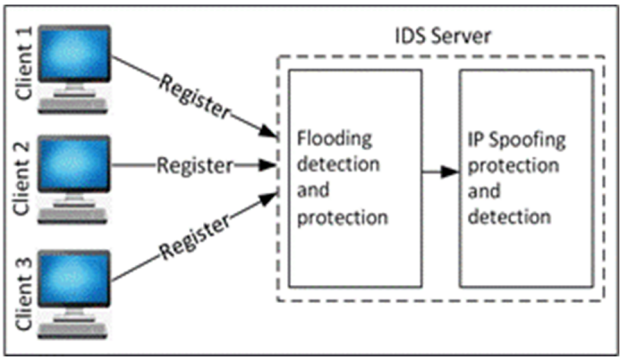


Figure 2. Components of Intrusion Detection System.

System Model involves IMS core roles involved in logging and session management procedures as shown in Figure 3. The signaling protocol for managing virtual media sessions is SIP. It provides versatility, making it easy for developers to integrate and deploy new services due to its text-based nature. But SIP makes the IMS environment vulnerable because it is defenseless against attacks such as DOS and DDOS. This work focuses on spoofing and register flooding attacks. During signaling flow for registration as a normal operation, UE must discover before registration the IP address of PCSCF, to which the user can submit the request. The request includes UE identity as well as a home network domain name. P-CSCF conducts DNS queries to find ICSCF in the home network. P-CSCF submits the request to ICSCF after the addition of details I-CSCF executes the selection procedure for S-CSCF then sent the application for registration to the chosen SCSCF. SCSCF considers the user illegal so it asks for HSS authentication data and sends a 401 unauthorized message to the user. UE assesses the response and sends the authentication information to P-CSCF with another register order. Once again P-CSCF finds I-CSCF and I-CSCF finds SCSCF in addition. SCSCF inspections responded to challenges. If the answer is right, then it accepts registration. The SCSCF takes the user profile from HSS and delivers a response of 200 OK to UE signifying positive registration. Zero watermarking scheme is used for detecting attacks of IP spoofing on IMS. Watermark is not directly embedded in the IP address rather, it is created by the use of IP address characteristics, thus preventing a great number of comparisons with already stored IP addresses and minimizing the subsequent delay. The method of watermarking includes embedding and extraction algorithms.

 doi:10.20944/preprints202401.1313.v1

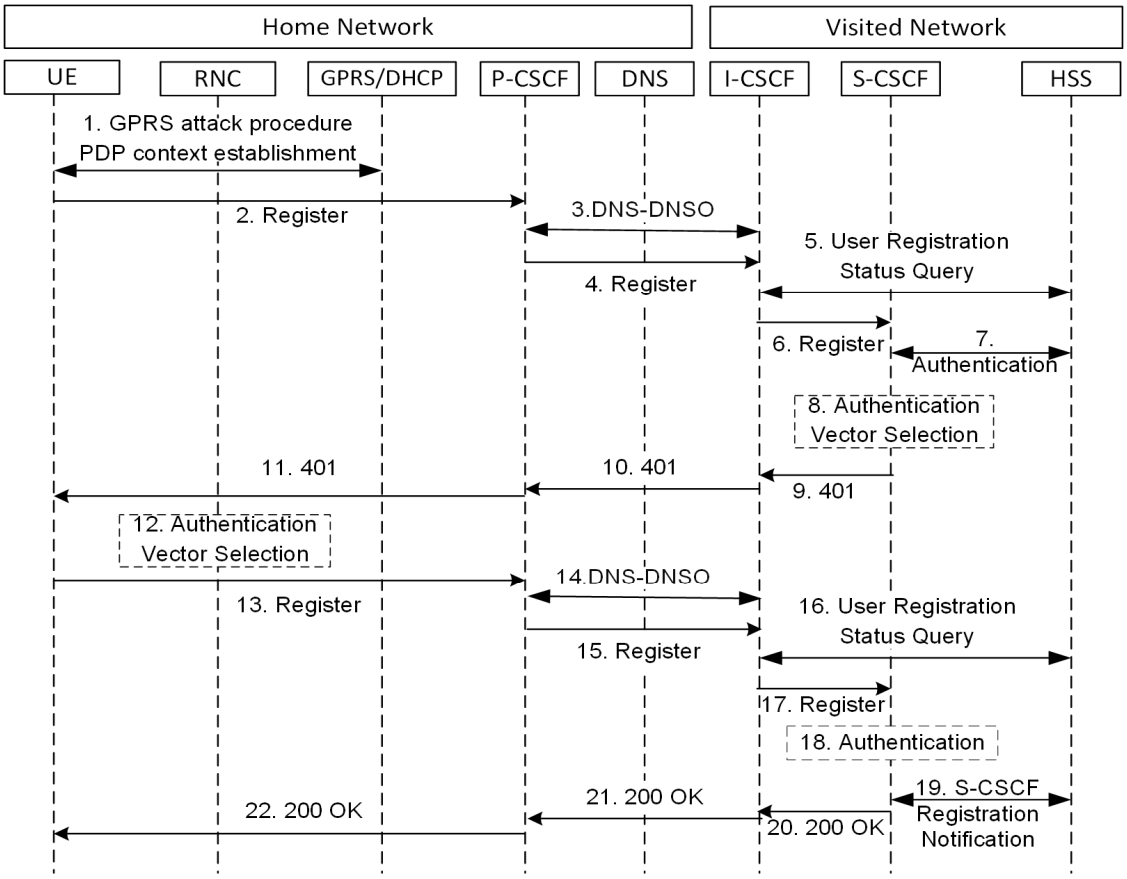


Figure 3. Registration Notification Process.

The KMC is a trusted authority in this method which the rightful owner registers a watermark. The flood detection and prevention method uses the principles of misuse and a hybrid anomaly detection algorithm that is based on zscore and cumulative sum to detect the flooding attack. Table 1 provides a list of the notations.

Table 1. List of Notations.

Notation	Description
Γ	Register request
B	Bandwidth
ξ (xi)	Threshold
ζ (zeta)	re-register
η (eta)	Reregistration list
ω(varpi)	Counter
ϱ (rho)	P-CSCF Load
Θ	Registration allowed
∞	De-register
UE	User Equipment
EK	
EBK	
FDPS	
KMC	Key Management Center
MLM	
MRR	
Mδ	

AY	
BL	Black List

The system identifies IP spoofing attacks on IMS to protect the network. The method of creating watermarking from the features of the IP address is done in 2 stages. The first one is algorithm embedding and the next is algorithm extraction. Watermark embedding is performed for proving copyright by the original creator and retrieval by KMC later. The KMC is a trusted authority in this method which the original owner registers his watermark with is a must requirement. We suggest using zero water labeling for IP address encryption

Intrusion Detection Protocol

1.UE embed $K_{IP,ID}$, *UE→ KMC:K*

2.UE→ KMC:γ *KMC extract K:*γ

*3.**If** EK==EBK **then** UE→ FDPS:*γ

*4.**Else** "Invalid Request"*

*5.**If*** $\gamma\ \beta \leq \xi$ ***then*** $\gamma \rightarrow BL$

*6.**Else*** $\gamma \rightarrow AY$ ***End If***

7.If $\gamma \equiv \zeta$, ***then*** $\gamma \rightarrow \eta$

*8.**Else*** $\gamma \rightarrow WL$ ***End If***

*9.**If*** $\gamma \in BL$ ***then*** Γ ++

*10**Else If*** $\gamma \in WL$ ***then*** $STATE\omega$++ ***EndIf***

*11.**If*** $\omega > 3$ // $\Gamma < 60$ ***then*** $\Upsilon \rightarrow BL$

*12.**Else*** $\omega \equiv 1$ ***End If***

13.IF$\rho \geq \xi$ ***then*** $MLM \leftarrow MRRM\delta$

14.IF $\delta \equiv$ *positive* ***then*** *inc* Γ *for BL*

15.set max $\vartheta\ \gamma \in \zeta \equiv 1$, *Set max* $\theta \equiv 1$

16.$\infty\ \gamma$ *whose* $\Gamma > 1$ ***EndIf***

A. Watermark Embedding Algorithm

The information is in a key, and the watermark is effectively embedded. The watermark embedding method is a digit sequence, where the original object (O) is a Register request including user parameters separated by a time (the partial key containing 3-digit group size and 2-digit cipher parameters). An embedding algorithm is used to fill the key. The algorithm does not make any adjustment to the request from the Log. In algorithm 1, the partial key constituents are shown, with a group size of three digits indicating the number of digits to be included in each group. The KMC then records the watermark, as well as the original IMPU value, keyword, current date, and time.

Algorithm 1: Watermark Embedding Algorithm

1. Enter the IP, γ.

2. IP and ID inputs are preprocessed.

3. Binary number B is assigned to each digit.

4.Coun tthe total number of digits(ND) in B

5. Take the group size (gpsize) and divide it into B groups using gpsizeNG (Number of groups) = ND/gpsize.

 doi:10.20944/preprints202401.1313.v1

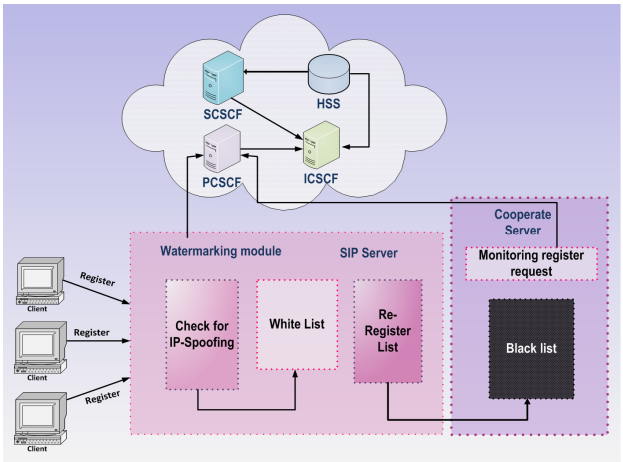
6. Determine the maximum number of 1s in each group and store them in MDL.

7. Create a key and a hash of the key.

8. Compress the key and γ.

Steps 1 and 2 shows that preprocessing removes special characters from the IP address of the registration client . In Step 3 alphabets are converted to binary. Steps 4 till 6 include that make groups of binary numbers of a specific size. Count the number of 1s in each group and save it in MD i.e. maximum digit list. MDL is a list that maintains the maximum number of 1s in each group against the group numbers.

Steps 7 and 8 give the key (K) as output that contains group size and MDL values. The key is hashed for security purposes and the original object and key are compressed.



B. *Extraction Algorithm*

The method is named as extraction algorithm that is responsible for extracting the watermark from the text. This algorithm accepts the request and the keyword for the register as input where the text may or may not be attacked. Using an extraction algorithm, the watermark is created from the text and it is compared with the original watermark that is registered with KMC. There could be multiple registrations of watermark that are distinguished by date and time of registration. The original author of a watermark is the one whose entry is old in KMC. In the absence of an attack on a register file, this technique accurately detects the watermark; the file is referred to as an authentic request.

Algorithm 2: Extraction Algorithm

1. Decompress key (K) and γ.

2. Calculate K's hash and compare it to the hash received.

3. Perform a pre-processing of the Register request (γ).

4. Each digit is translated into its binary equivalent.

5. Count the total number of digits(ND) in B.

6. Read the group size (gpsize) and create B groups depending on it, i.e. *NG (Number of groups) = ND/gpsize.*

7. Generate MDL by identifying the most often occurring digit 1 in each group.

8. Watermark (W) taken from the output.

 doi:10.20944/preprints202401.1313.v1

In Steps 1-4, The first step is to decompress O and key. For comparison, Hash is created from O and Key, then all special characters are deleted from the parameters of the request register. Increasing alphabet is translated to its numerical equivalent then each digit is converted to its binary equivalent. Steps (5)-(8) discuss group formation dependent on group size. In this step the frequency of each numerical digit (1) counts in each group and the maximum numerical digit 1 occurring in each group is defined. By using the main (K) watermark is obtained from the text. The reversed process of embedding and encryption, as outlined in the extraction procedure, is used to create a watermark. The following are the main guidelines that must be followed in the event of an emergency during the registration process: i) Users are not permitted to send more than one Register and re-register request within 60 seconds if an attack is detected. ii) When the critical number of registrations exceeds 2/sec, all users already in the WL de-register. Otherwise, the re-registration value increases from 2/sec. These instructions are executed as follows; i) inc γ for BL-γ; ii) set max $\eth\ \gamma \in \zeta \equiv 1$ and iii) set max $\theta \equiv 1, \gamma > 1$. The cooperative server's major component is MRRM, which tracks the number of register requests that traverse P-CSCF, which will increase while the number of 200 OK responses decreases during flood attacks. The difference between register request and 200 OK answer in normal behavior is nearly zero, and it will be further improved. According to this function, by observing the difference, we can detect the register flood. A positive value is sent IDS for π>200 OK and πIDS if the value of the difference is abruptly modified (not zero), indicating that a flooding attack has occurred. As soon as IDS starts receiving requests for registers, the control of bandwidth is disabled, i.e. π IDS is disabled. Whenever a user transfers parameters to have his bandwidth tracked registered. If the bandwidth level used by any IP exceeds the level cap, the request for the register is considered an infringement, and the user is denied. The threshold is set at 225 bytes because that is the size of the SIP registration file. When the consumer reaches by more than 280 the violation will be viewed. Therefore, for a certain duration, the program will push this IP into blacklist, based on how dangerous is the intruder. The register request is received after the bandwidth monitoring module has been checked and a reregister message is received, it is forwarded to the re-register list. A reregistered list contains counter requests for re-registration for the already registered UE. The number of times IP with the counter value is re-registered in a second is processed. For instances where an attacker's IP is first identified, it is applied to the blacklist where a period for deletion is also started. It is auto-deleted from the blacklist after the threshold deletion period of some IP has expired. Similarly, if an attacker's IP is identified again before its deletion time expires, then its deletion time is changed and increased based on its attack severity level. The mechanism of updating the timeframe of deletion and auto-deletion from the blacklist is defined as $\gamma \in$BL,γ++.

Assume IP doesn't work in BL, it is tested in WL. If it is not contained in it, then add it to WL and a counter value 1 is added to the counter in the form of мWL, π<60, π1. If an already registered user sends a register message in 60 seconds three times, then it is deleted from the WL and placed in BL for a certain period. If an IP is suspicious then the IDS first checks in the BL to secure the device. If the attacker's IP address does not already exist in the BL, it is created and a deletion time is set. If the attacker's IP is already in the BL, then it signifies the IP as attempted to attack previously. To counteract, IDS enhances the deletion time IP, ω>3, γ<60, $\gamma \rightarrow$BL.

4. Results and Analysis

To determine IDS output for authentication and reauthentication operations, we assess the proposed IDPS detection rate where IMS testbed is implemented as shown in Figure 4. The Fokus IMS Core was built on the server and the contact used an open-source IMS application from Boghe. The IMS software was built on a 2.4 GHz Intel Core i3 computer with 4 GB of RAM, while the client was mounted on a 2.4 GHz Intel Core i5 with 4 GB of RAM. We design and optimize the Audio / Video calling Fokus IMS Core among two users as well as the calling to the meeting. All services which include registration \ authentication, voice call, video call, conference call, etc. are checked. The IMS Core was reconfigured according to the findings and again checked for validation. Next, it introduced the main security framework with two servers namely the IDS server and the cooperative server. Before rerouting the request to the main IMS server, it was built to make client requests and minimize security threats. A SIP traffic generator known as the SIPp is used for research to produce flood traffic. While using the Testbed we assess authentication response time and through subsequent re-authentication. Next, we test the detection of registry flooding requests, Processor load, error detection ratio, and memory utilization.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 18 January 2024 doi:10.20944/preprints202401.1313.v1

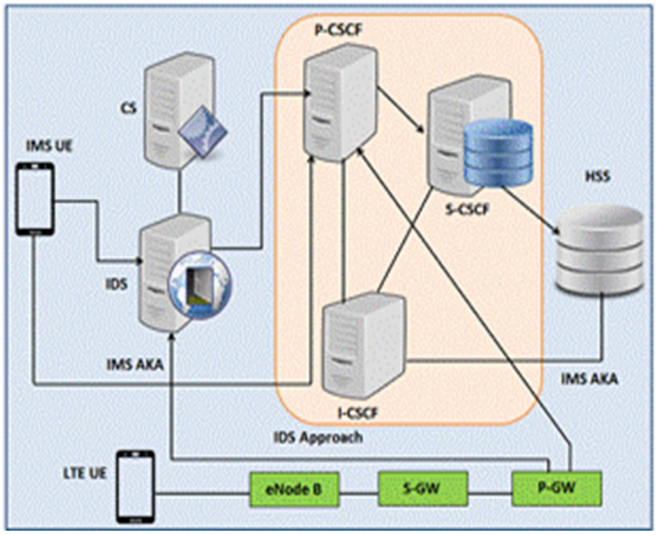


Figure 4. Deployment Scenario for Testbed.

Major baseline approaches deployed in the testbed are PIKE [33], IDS-IVS [48], SSI [49], and DS-IDP [5] Following scenarios are considered during the registration process; i) In this case, a request generator (RG) produces traffic of 50 SIP REGISTER requests per second, the response time for authentications is observed; ii) Response time comparison with current IMS authentication procedure; iii) Term span during which traffic is tracked is split into 3 periods, the test scenarios for identification are considered from 20 seconds to a minute; iv) The time during which traffic is tracked is split into 4 periods, the measurement scenarios for the identification duration are known to be about 15 seconds over a minute.

A. Response time

Response time is the amount of time it takes for IMS Servers to deliver user responses against Register requests. The response time is influenced by variables like network bandwidth, the number of users, the number and type of requests sent, and mean processing time. In this experiment, the total delay during device performance measurement measures the time is taken to fulfill a register request and return the average response time of all requests The response time is measured for standard IMS (CONVIMS), IDS-IVS, DS IDP, and proposed IDPS, which is performed to see the effect of adding a new IDS module, and the time user has to wait for a response. The quicker the response time, the more requests are handled every minute. Scenarios S1 is used to determine the change in reaction time triggered by the introduction of IDS module in front of the core entities of IMS. Here, after 60 seconds, the results seen in the 50 IMS app authentication questions are sent 10 times each. Figure 5(a) clarifies the delay imposed on the Registered Requests because of the IDS feature. It is low since nearly all calculations were performed within a millisecond. The response time in the proposed IDPS is determined using RT=((n-r))/Tp , where n is the number of users or is the number of requests received by IDS server, Tp is the Total processing time by IMS core entities and IDPS. Figure 5(b) elucidates the time of execution for embedding the watermark at the sender and the receiver retrieval. Statistics reveal that the embedding time for 6 requests is 0.062 μ seconds and the extraction time 0.025 μ seconds.

 doi:10.20944/preprints202401.1313.v1

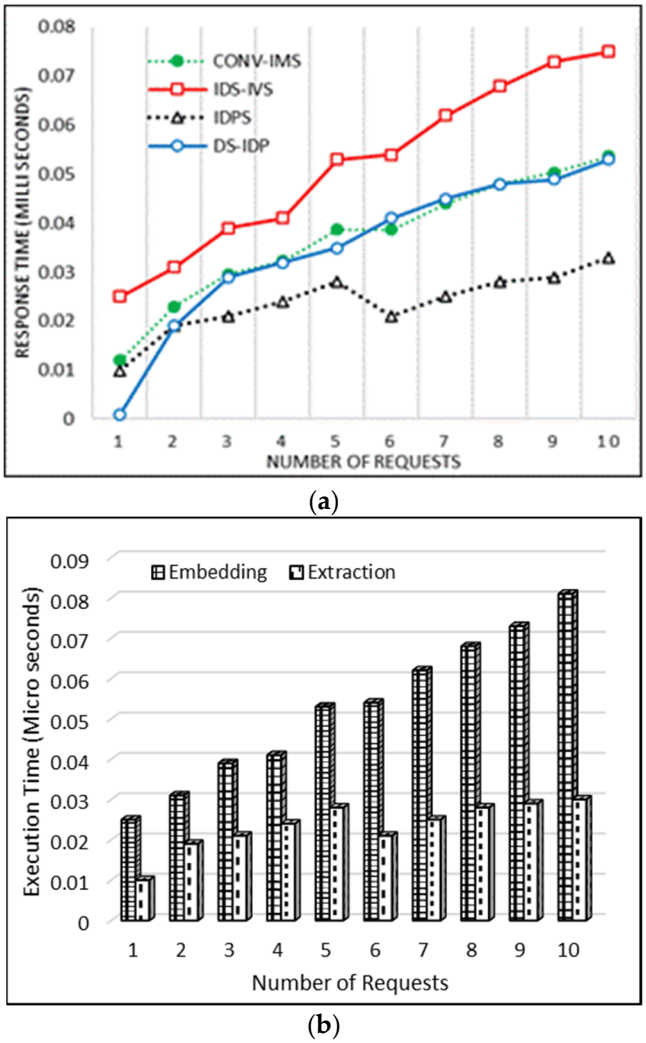


Figure 5. Response Time in (a) and execution time in (b) for different numbers of requests.

B. Detection Algorithm for Register Flooding

The CUSUM and zscore detection algorithm map PCSCF traffic and identify the MLM attack. Table 2 displays the normal, peek and attack traffic values which are calculated for specific request numbers using the CUSUM and zscore detection algorithm. In the first experiment, the genuine user is first identified via IMS app. The IDS, after updating its WL record, will forward this client to P-CSCF for registration. Only one UE is active in this situation, therefore CLMM observes low Processor load on PCSCF. Figure 6(a) indicates the CPU load on PCSCF to register effectively during normal traffic. There were 50 attackers in the second case who attempt to submit illegal requests for databases. It results in 60 requests per second and in turn, amounts to 480 unwanted messages which is a large number of messages to waste CPU power which sets up an attack situation and the threshold is crossed. IDS needs to check that it is not a false warning by calling CS information that checks the uncertainty of the register question and that the response of 200 OK has to be below zero when it was very high. It supports the assault by the historical flood. Figure 6(b) elucidates the CPU load on PCSCF under registry flooding attack. A large number of authenticated messages are stored in the actual PCSCF world. Therefore, efficiency must not be affected since two servers are installed in the proposed IDPS. In both regular and high traffic circumstances, the findings presented lowered the average delay per message.

 doi:10.20944/preprints202401.1313.v1

Table 2. Traffic Analysis.

NMI	Z_n	Normal Traffic	Peak Traffic	Attack Traffic
30	9.34	60	80	200
50	11	100	140	261
100	16	200	300	400
500	19	1400	1500	2400

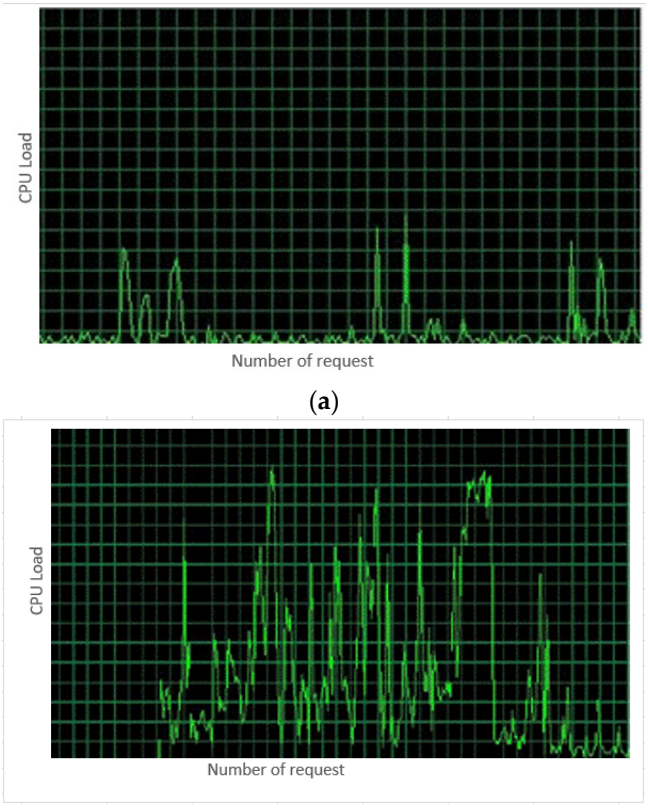


Figure 6. CPU load on P-CSCF for normal scenario is presented in (a) and under attack scenario is shown in (b).

C. CPU Load Utilization

CPU load refers to the use of computer processing power or the volume of work that a CPU performs. The realistic use of the CPU differs in the feature of quantity and the nature of controlled computing activities. The performance of PCSCF may be affected by the CPU load of different IDS schemes. When monitoring Processor load for PCSCF, if it exceeds the threshold value then the CS server is asked to validate the details. In the case that the CS server sends positive value parameter π, the flood attack is alarmed. As a consequence, emergency rules are implemented in the form of π Get π.

Therefore, the IDS is placed before the core of IMS in the proposed solution, core server work is less effective. However, if an external module is introduced it affects CPU load, a different IDS module was installed under the new IDPS solution instead of being introduced on existing servers. The load of CPUs is observed at PCSCF with and without DS-IDPS by submitting requests from the legal and malicious client in the range of 10 to 3500 requests at a time. Figure 7(a) indicates CPU load as up to 3500 requests on PCSCF range in the amount of requests. It considers a case where for the original IMS IDS is not attached between PCSCF and device. Once IDS is connected, it always shows the scenario as in the foundation schemes. CPU load tends to keep rising at PCSCF as the number of requests grows. In original IMS, if several further requests are sent to P-CSCF, then a Denial of Service (DoS) attack might occur. Figure 7(b) elucidates the pressure on the CPU over an 8 second time

 doi:10.20944/preprints202401.1313.v1

period. The CPU load depends on the number of incoming requests in each scheme. Statistics reveal that, when a significant number of messages are sent, no DSIDP in original IMS and PIKE crosses up to 80 percent and 50 percent in just 6 seconds. In a few seconds, it can reach up to denial of service. DSIDP and planned IDPS have a CPU load of up to 20 percent and 18 percent It can handle the message storm for furthermore time as compared to counterparts.

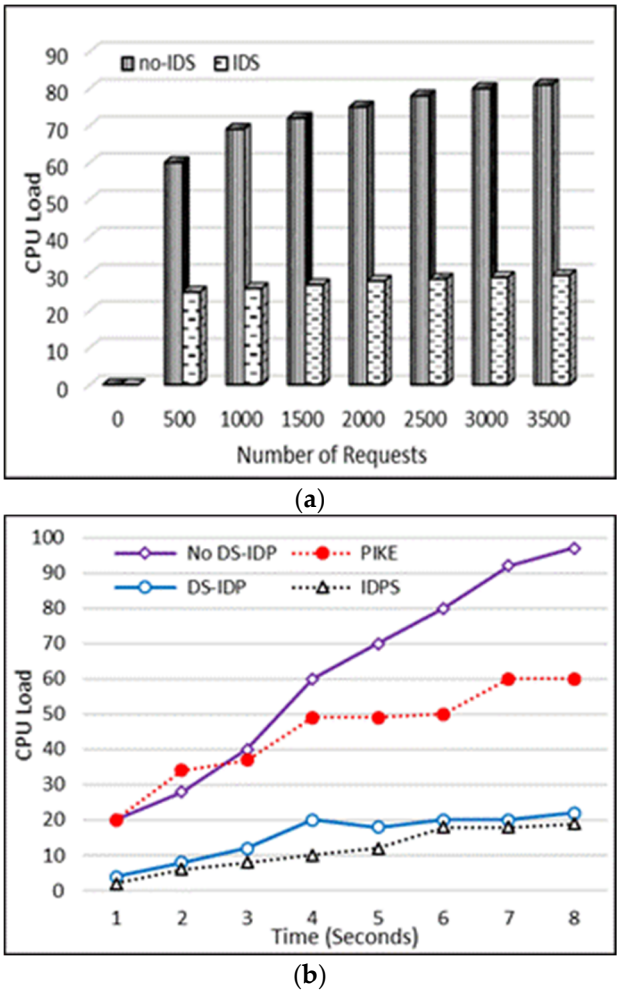


Figure 7. CPU Load for number of requests for IDS and non-IDS scenario is presented in (a) and Time comparision of proposed and previous schemes is shown in (b).

D. Fault Detection Ratio

A particular number of requests (RF) are forged during the fault detection process where the number of requests detected (RD) is measured out of the total number of requests received. The ratio of fault detection is determined as $F_{DR} = R_F \setminus FR_D$. Figure 8 shows that detection accuracy for low-intensity attacks improves with fewer requests, while the detection accuracy of high-intensity attacks decreases with fewer requests. While attacks do not display the same degree of identification accuracy for a greater number of requests, high-impact attacks are detected for reasonable precision. Since it could be analyzed that when the intensity is 1000 and the number of requests is 40, however, the accuracy rate of the proposed IDPS is 100%, PIKE gives 83 % accuracy, VA gives 90.94% accuracy and SSI is 92% accuracy.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 18 January 2024 doi:10.20944/preprints202401.1313.v1

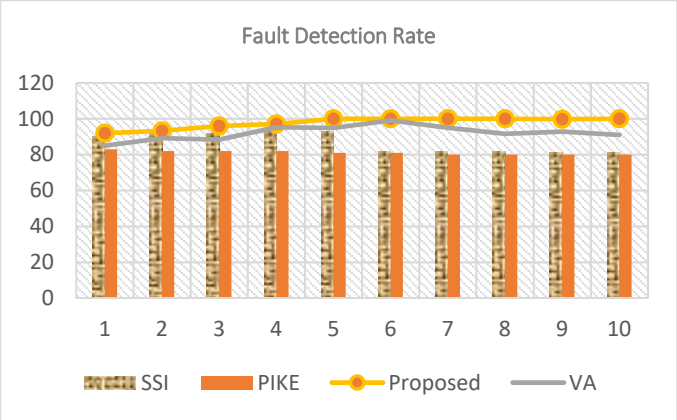


Figure 8. Fault-detection ratio.

E. Memory utilization

Memory is the storage area of the CPU, and the use of storage indicates the volume of memory the Processor retains for computation. On PCSCF the use of memory is interpreted by submitting different quantities of registration requests. Figure 9 shows memory usage on P-CSCF without the execution of an IDPS. This shows that memory usage hit up to 80 percent when making 2000 registration requests. If the number of applications sent to PCSCF increased, it may be as high as 100%. Usage of memory on PCSCF by applying the IDPS introduced before PCSCF. For the same number of requests, i.e. 2000, resource use is just 35 percent.

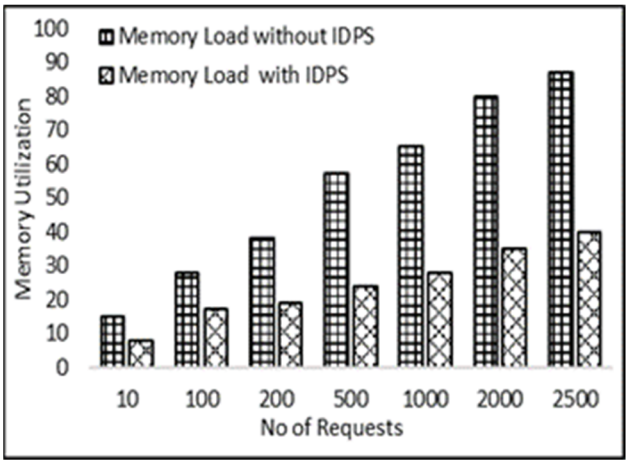


Figure 9. CPU load for different attack rates.

5. Conclusions

In this paper, we present a scheme that detects and prevents the IMS network from flooding and spoofing attacks. An IDS is configured where a pair of subsystems run, one is a spoofing subsystem for identification and prevention, and the other is a flood identification and prevention subsystem. The spoofing attack is observed by zero scheme. Since watermark is not contained in the IP address itself, it is created by the use of IP address characteristics, thereby preventing a large number of comparisons with previously stored IPs and reducing the resulting delay. The method of watermarking includes two stages of algorithm embedding and algorithm extraction. Watermark embedding is performed for claiming ownership by the original author and extraction by KMC later. The flood detection system operates on rules of misuse and anomaly detection algorithms to provide IMS and VOLTE environments with effective detection and prevention. Results show the superiority of the proposed IDPS over predecessors in terms of response time, attack detection ratios, Processor

 doi:10.20944/preprints202401.1313.v1

load, fault detection ratio, and memory consumption. We shall evaluate the impact of IDS in the future during massive multimedia data exchange from 5 G and 6 G smart devices.

6. Threat Analysis:

a. Resistance to IP-Spoofing attack

The IP-address of the client is watermarked using zero water marking then the information of watermark is forwarded with the regiter request that is extracted at the IDS before forwarding to PCSCF

b. Resistance to flooding attack

The proposed system intrusion detection system avoids the flooding attack and if any IP floods the regiteration requests it is forwarded to blacklist

The cooperative server's major component is MRRM, which tracks the number of register requests that traverse P-CSCF, which will increase while the number of 200 OK responses decreases during flood attacks. The difference between register request and 200 OK answer in normal behavior is nearly zero, and it will be further improved. According to this function, by observing the difference, we can detect the register flood. A positive value is sent IDS for π>200 OK and πIDS if the value of the difference is abruptly modified (not zero), indicating that a flooding attack has occurred

References

1. Park, R. Jin Ho, S. Shailendra, S. Sushil Kumar, E. A. Mikail Mohammed, W. K. Abir, Y. P. P. Tae and J. Hyuk, "A Comprehensive Survey on Core Technologies and Services for 5G Security: Taxonomies, Issues, and Solutions," *Human-centric Computing and Information Sciences,* vol. 11, no. 3, 2021.
2. Siddiqu, A. F and H.U.A, "Dual server based security system for multimedia Services in Next Generation Networks," *Multimedia Tools and Applications,* pp. 1-20, 2019.
3. S. a. N. M. Armoogum, "Sorted Galloping Prevention Mechanisms Against Denial of Service Attacks in SIP-Based Systems," *Progress in Advanced Computing and Intelligent Engineering,* pp. 571-583, 2021.
4. J. Manan, A. Ahmed, I. Ullah, L. Merghem-Boulahia and D. Gaïti, "Distributed intrusion detection scheme for next generation networks," *Journal of Network and Computer Applications,* vol. 147, 2019.
5. N. Ruan, M. Wu, S. Ma, H. Zhu, W. Jia and S. Wu, "Detect and Prevent SIP Flooding Attacks in VoLTE by Utilizing a Two-Tier PFilter Design," *IEICE Transactions on Information and Systems,* vol. E100–D, no. 10, pp. 2287-2294, 2017.
6. Siddiqui, A. Faria Jan, U. Humaira and Ata, "Dual server based security system for multimedia Services in Next Generation Networks," *Multimedia Tools and Applications,* vol. 79, no. 11, pp. 7299-7318, 2020.
7. Xiaolong and Huang, "Network Intrusion Detection Based on an Improved Long-Short-Term Memory Model in Combination with Multiple Spatiotemporal Structures," *Wireless Communications and Mobile Computing,* 2021.
8. M. Umer and M. B. Y. Sher, "A two-stage flow-based intrusion detection model for next-generation networks," *PLoS ONE 13(1):* , vol. 13, no. 1, 2018.
9. J. Fajardo, F. Liberal, F. Li, N. Clarke and I.-H. Mkwawa, " End-to-middle-to-end solution for IMS media plane security. 19, (2019)," *Electronic Commerce Research* , vol. 19, p. 719–746, 2019.
10. A. Ghani, E. H. Ibn-Elhaj and A. Hammouch, "Quality Adaptation by Using Scalable Video Coding (SVC) over P2P IP Multimedia Subsystem (P2P IMS)," in *Proceedings of the 2nd International Conference on Networking, Information Systems & Security*, Rabat, Morocco, 2019.
11. M. A. Azad, S. Bag, C. Perera, M. Barhamgi and F. Hao, "Authentic Caller: Self-Enforcing Authentication in a Next-Generation Network," *IEEE Transactions on Industrial Informatics,*, vol. 16, no. 5, pp. 3606-3615, 2020.
12. Tahira, U. Shireen, A. Ata, S. Humaira and Muhammad, "Efficient Security Associations Establishment Using IPSec in IMS after Handover in NGMN," *Journal of Internet Technology,* vol. 20, no. 2, 2019.
13. M. Naeem, H. Makhdoom, M. S. M. Intesab and Malik, "A survey on registration hijacking attack consequences and protection for Session Initiation Protocol (SIP)," *Computer Networks,* vol. 175, p. 107250, 2020.
14. Jawad and Nawar, "Mobile Edge Cloud: Intelligent deployment and services for 5G Indoor Network," Brunel University London, 2021.

15. K. Nina and K. Anastasia, "Quality of services evaluation method in next generation networks," in 14th International Conference on Advanced Trends in Radioelecrtronics, Telecommunications and Computer Engineering (TCSET), pp. 1055–1058, , Lviv-Slavsk, 2018.
16. H. Kilinc and T. Yanik, "A survey of SIP authentication and key agreement schemes.," *Communications Surveys & Tutorials, IEEE,* pp. 1005-1023., 2014.
17. B. Koo, S. Kim and H. Kim, "Security and Countermeasures against SIP-Message-based Attacks on the VoLTE," in 19th International Conference in Communications, part of 19th International Conference on Circuits, Systems, Communications and Computers (CSCC 2015), pp.132–135, Zakynthos Island, Greece, 2015.
18. Y. e. a. Wu, "Intrusion detection in voice over IP environments.," *Int. J. Inf. Secur.8,* , p. 153–172 , 2009.
19. R. Safoine, S. Mounir and A. Farchi, "Comparative study on DOS attacks Detection Techniques in SIP-based VOIP networks," in *6th International Conference on Multimedia Computing and Systems (ICMCS), pp. 1–5*, Rabat., 2018).
20. H. e. a. Abdelnur, "Abusing SIP authentication.," 2008.
21. N. e. a. Asokan, " Man-in-the-middle in tunnelled authentication," *Lecture Notes in Computer Science, vol. 3364,* , p. p. 28, 2005.
22. A. Forte, W. Wang, L. Veltri and G. Ferrari, "A Next-Generation Core Network Architecture for Mobile Networks.," *Future Internet,* vol. 11, no. 7, 2019.
23. D. e. a. Sisalem, SIP Security, Wiley, 2009.
24. M. Y. &. T. C. H. Su, "An Approach to Resisting Malformed and Flooding Attacks on SIP Servers.," *Journal of Networks, 10(2),,* pp. 77-84., 2015.
25. A. &. P. A. R. Bansal, "Mitigation of Flooding Based Denial of Service Attack against Session Initiation Protocol Based VoIP System.," in *In Computational Intelligence & Communication Technology (CICT), IEEE International Conference on*, 2015, February..
26. Muhammad Morshed Alam, Muhammad Yeasir Arafat, Feroz Ahmed, "Study on Auto Detecting Defence Mechanisms against Application Layer Ddos Attacks in SIP Server," *Journal of Networks,* vol. 10, no. 6, pp. 344-352, Jun 2015.
27. A. Bansal and R. Alwyn, "Mitigation of Flooding Based Denial of Service Attack against Session Initiation Protocol Based VoIP," in *IEEE International Conference on Computational Intelligence & Communication Technology*, 2015.
28. Dahham Allawi, Alaa Aldin Rohiem, Ali El-moghazy and Ateff Ghalwash, "New Algorithm for SIP Flooding Attack Detection," *International Journal of Computer Science and Telecommunications,* vol. Volume 4 , no. Issue 3, pp. 10-19, March 2013.
29. Jakub Safarik*, Jiri Slachta, "VoIP attacks detection engine based on Neural Network," in *Proc. SPIE 9496*, 20 May 2015.
30. L. Manunza, S. Marseglia and S. Romano, "Kerberos: a real-time fraud detection system for IMS-enabled VoIP networks. J Netw Comput Appl," *Journal of Network and Computer Applications,* vol. 80, p. 22–34, 2017.
31. H. Sengar, H. Wang, D. Wijesekera and S. Jajodia, "Detecting VoIP Floods Using the Hellinger Distance," *IEEE Transactions on Parallel and Distributed Systems,* vol. 19, no. 6, pp. 794-805, 2008.
32. E. Chen and M. Itoh, "A whitelist approach to protect SIP servers from flooding attacks," in *IEEE International Workshop Technical Committee on Communications Quality and Reliability (CQR)*, Vancouver, BC, 2010.
33. K. Jonguk, B.-h. Roh, M. Hong and S. Kang, "Autonomous Defense against Flooding-based Denial of Service of a SIP System," in *Applications and Technology Conference (LISAT), 2010 Long Island Systems*, Farmingdale, NY, 2010.
34. Wenhai Li, Wei Guo, Xiaolei Luo, Xiang Li, "On Sliding Window Based Change Point Detection for Hybrid SIP DoS Attack," in *Services Computing Conference (APSCC), 2010 IEEE Asia-Pacific*, Hangzhou, 6-10 Dec. 2010.
35. Jin Tang , Yu Cheng, "Quick Detection of Stealthy SIP Flooding Attacks in VoIP Networks," in *Communications (ICC), 2011 IEEE International Conference on* , Kyoto , 5-9 June 2011 .
36. Sven Ehlert* , Ge Zhang , Dimitris Geneiatakis , Georgios Kambourakis , Tasos Dagiuklas ,Jiřˇí Markl , Dorgham Sisalem, "Two layer Denial of Service prevention on SIP VoIP infrastructures," *Computer Communications,* vol. 31, no. 10, p. 2443–2456, 25 June 2008.
37. A. M.A, Z. Tariq and M. Farooq, "A comparative study of anomaly detection algorithms for detection of SIP flooding in IMS," in *2nd International Conference on Internet Multimedia Services Architecture and Applications (IMSAA)*, Bangalore, 2008.
38. Jens Fiedler, Tomas Kupka, Sven Ehlert, Prof. Dr. Thomas, Dr. Dorgham Sisalem, "VoIP defender: highly scalable SIP-based security architecture," in *IPTComm '07 Proceedings of the 1st international conference on Principles, systems and applications of IP telecommunications*, New York, 2007.

39. H. Shoket and J. Aulakh, "Secure VOIP LTE network for secure transmission using PLRT (Packet Level Restraining Technique) under DDOS Attack," in *5th International Conference on Signal Processing and Integrated Networks (SPIN), pp. 878-88*, Noida, 2018.
40. Mitra Alidoosti, Hassan Asgharian, Ahmad Akbari, "Security framework for designing SIP scanner," in *Electrical Engineering (ICEE), 2013 21st Iranian Conference on* , Mashhad , May 2013 .
41. S. Marchal, A. Mehta, V. Gurbani, R. State, T. Ho and F. Sancier-Barbosa, "Mitigating mimicry attacks against the Session Initiation Protocol (SIP)," *IEEE Transactions on Network and Service Management*, vol. 12, no. 3, 2015.
42. Neda Hantehzadeh, Anil Mehta, Vijay K. Gurbani, Lalit Gupta, Tin Kam Ho, Gayan Wilathgamuwa, "Statistical analysis of self-similar Session Initiation Protocol (SIP) messages for anomaly detection," in *New Technologies, Mobility and Security (NTMS), 2011 4th IFIP International Conference on*, Paris, 7-10 Feb. 2011.
43. Anil Mehta, Neda Hantehzadeh, Vijay K. Gurbani, Tin Kam Ho, Flavia Sancier, "On using multiple classifier systems for Session Initiation Protocol (SIP) anomaly detection," in *Communications (ICC), 2012 IEEE International Conference on*, Ottawa, ON, 10-15 June 2012.
44. Anil Mehta, Neda Hantehzadeh, Vijay K. Gurbanit, Tin Kam Hot, Jun Koshiko,Ramanarayanan Viswanathan, "On the inefficacy of Euclidean classifiers for detecting self-similar Session Initiation Protocol (SIP) messages," in *Integrated Network Management (IM), 2011 IFIP/IEEE International Symposium on*, Dublin, 23-27 May 2011.
45. M. Z. Rafique, F. Ahmet, M. K. Khan and M. Farooq, "Securing Smart Phones Against Malicious Exploits.," *International Information Institute (Tokyo). information*, vol. 15, no. 2, pp. 903-912, 2012..
46. H. Intesab, S. Djahel, D. Geneiatakis and F. Naït-Abdesselam, "A lightweight countermeasure to cope with flooding attacks against session initiation protocol," in *Wireless and Mobile Networking Conference (WMNC),*, 2013.
47. N. a. C. L. Vrakas, "An intrusion detection and prevention system for IMS and VoIP services," *International Journal of Information Security*, vol. 12, no. 3, pp. 201-2017, 2013.
48. D. Khaled, S. Haidar, H. Abbas and E.-H. Wassim, "A SIP delayed based mechanism for detecting VOIP flooding attacks," in *International Wireless Communications and Mobile Computing Conference (IWCMC), pp. 588–593*, Cyprus, Paphos, 2016.
49. Ashraf, U. Humaira, T. Ata, S. Shireen and Muhammad, "Efficient Certificate Based One-pass Authentication Protocol for IMS," *Journal of Internet Technology*, vol. 20, no. 4, pp. 1133-1143, 2019.
50. Oladimeji and Deborah, "An Intrusion Detection System for Internet of Medical Things," Dalhousie University, Halifax, Nova Scotia, 2021.
51. J. H. Pacheco, B. C. Victor, S. Luis. Felix-Herran and Pratik, "Artificial neural networks-based intrusion detection system for internet of things fog nodes," *IEEE Access*, pp. 73907-73918, 2020.
52. A. S. Jain, S. Tanya, P. Satyendra K. and Vikas, "Implementing Security in Iot Ecosystem using 5G Network Slicing and Pattern matched Intrusion Detection System: A Simulation Study," Interdisciplinary Journal of Information, Knowledge & Management, vol. 16, 2021
53. Lim, M., Abdullah, A., Jhanjhi, N. Z., Khan, M. K., & Supramaniam, M. (2019). Link prediction in time-evolving criminal network with deep reinforcement learning technique. IEEE Access, 7, 184797-184807.
54. Humayun, M., Ashfaq, F., Jhanjhi, N. Z., & Alsadun, M. K. (2022). Traffic management: Multi-scale vehicle detection in varying weather conditions using yolov4 and spatial pyramid pooling network. Electronics, 11(17), 2748.
55. Gaur, L., Singh, G., Solanki, A., Jhanjhi, N. Z., Bhatia, U., Sharma, S., ... & Kim, W. (2021). Disposition of youth in predicting sustainable development goals using the neuro-fuzzy and random forest algorithms. Human-Centric Computing and Information Sciences, 11, NA.
56. Shahid, H., Ashraf, H., Javed, H., Humayun, M., Jhanjhi, N. Z., & AlZain, M. A. (2021). Energy optimised security against wormhole attack in iot-based wireless sensor networks. Comput. Mater. Contin, 68(2), 1967-81.
57. Ghosh, G., Verma, S., Jhanjhi, N. Z., & Talib, M. N. (2020, December). Secure surveillance system using chaotic image encryption technique. In IOP conference series: materials science and engineering (Vol. 993, No. 1, p. 012062). IOP Publishing.
58. Gaur, L., Afaq, A., Solanki, A., Singh, G., Sharma, S., Jhanjhi, N. Z., ... & Le, D. N. (2021). Capitalizing on big data and revolutionary 5G technology: Extracting and visualizing ratings and reviews of global chain hotels. Computers and Electrical Engineering, 95, 107374.
59. Almusaylim, Z. A., Zaman, N., & Jung, L. T. (2018, August). Proposing a data privacy aware protocol for roadside accident video reporting service using 5G in Vehicular Cloud Networks Environment. In *2018 4th International conference on computer and information sciences (ICCOINS)* (pp. 1-5). IEEE.
60. Adeyemo, V. E., Abdullah, A., JhanJhi, N. Z., Supramaniam, M., & Balogun, A. O. (2019). Ensemble and deep-learning methods for two-class and multi-attack anomaly intrusion detection: an empirical study. *International Journal of Advanced Computer Science and Applications*, *10*(9).

 doi:10.20944/preprints202401.1313.v1

61. Wassan, S., Chen, X., Shen, T., Waqar, M., & Jhanjhi, N. Z. (2021). Amazon product sentiment analysis using machine learning techniques. *Revista Argentina de Clínica Psicológica*, *30*(1), 695.
62. Pal, S., Jhanjhi, N. Z., Abdulbaqi, A. S., Akila, D., Almazroi, A. A., & Alsubaei, F. S. (2023). A hybrid edge-cloud system for networking service components optimization using the internet of things. Electronics, 12(3), 649.