electronics

MDPI

Article

Detecting Nuisance Calls over Internet Telephony Using Caller Reputation

Ibrahim Tariq Javed [1,*], Khalifa Toumi [2], Fares Alharbi [3], Tiziana Margaria [1] and Noel Crespi [4]

[1] The Irish Software Research Centre (LERO), University of Limerick, V94 T9PX Limerick, Ireland; tiziana.margaria@lero.ie
[2] IRT SystemX, Paris-Saclay, 91127 Palaiseau, France; khalifa.toumi@irt-systemx.fr
[3] Department of Computer Science, Shaqra University, Shaqra 15526, Saudi Arabia; faalhrbi@su.edu.sa
[4] Institut Mines-Télécom, Télécom SudParis, 91011 Evry CEDEX, France; noel.crespi@mines-telecom.fr
* Correspondence: Ibrahimtariq.javed@lero.ie

Abstract: Internet telephony permit callers to manage self-asserted profiles without any subscription contract nor identification proof. These cost-free services have attracted many telemarketers and spammers who generate unsolicited nuisance calls. Upon detection, they simply rejoin the network with a new identity to continue their malicious activities. Nuisance calls are highly disruptive when compared to email and social spam. They not only include annoying telemarketing calls but also contain scam and voice phishing which involves security risk for subscribers. Therefore, it remains a major challenge for Internet telephony providers to detect and avoid nuisance calls efficiently. In this paper, we present a new approach that uses caller reputation to detect different kinds of nuisance calls generated in the network. The reputation is computed in a hybrid manner by extracting information from call data records and using recommendations from reliable communicating participants. The behavior of the caller is assessed by extracting call features such as call-rate, call duration, and call density. Long term and short term reputations are computed to quickly detect the changing behavior of callers. Furthermore, our approach involves an efficient mechanism to combat whitewashing attacks performed by malicious callers to continue generating nuisance calls in the network. We conduct simulations to compute the performance of our proposed model. The experiments conclude that the proposed reputation model is an effective method to detect different types of nuisance calls while avoiding false detection of legitimate calls.

Keywords: VoIP; SPIT; voice-spam; nuisance call; reputation; trust

Citation: Javed, I.T.; Toumi, K.; Alharbi, F.; Margaria, T.; Crespi, N. Detecting Nuisance Calls over Internet Telephony Using Caller Reputation. *Electronics* **2021**, *10*, 353. https://doi.org/10.3390/electronics10030353

Academic Editor: Nour Moustafa
Received: 17 December 2020
Accepted: 27 January 2021
Published: 2 February 2021

1. Introduction

Internet Telephony has revolutionized our communication way. Solutions like Skype, Whatsapp, and Viber offer globally accessible, cost-effective, flexible, and convenient communication services. Furthermore, WebRTC [1] has facilitated context-based communication where information and conversational data related to the same context are provided together. Novel VoIP platforms based on WebRTC have enabled features of cross-domain interoperability and identity portability [2]. The major factor contributing to the growth of the Internet telephony market is its price performance. Moreover, Internet telephony is capable of providing rich media, service mobility, integrated applications, user control interface, and other enhanced features. Internet telephony services are easy to install, use, and troubleshoot. Therefore, the market of VoIP call services is forecast to increase to the US $194.5 billion by 2024 [3].

Despite the advantages, several threats are associated with Internet telephony [4] as categorized in the threat taxonomy presented in Figure 1. They can be broadly classified into integrity, availability, confidentiality, and social threats. Confidentially threats involve unauthorized access to information such as media eavesdropping and call pattern tracking. Integrity threats are the alteration of signals or the message by intercepting it from the

network. Availability threats are in the form of denial of service attacks that aim to disrupt the availability of the service such as call flooding and protocol fuzzing. A social threat is different from other technical threats in terms of intention and methodology. It focuses on the manipulation of the social context between communication parties to attack the victim. These threats are realized over Internet telephony by generating nuisance calls. Nuisance calls are spam calls generated in an unsolicited manner over the network. Nuisance calls are viewed as considerably more troublesome than messages or social spam since calls are produced in real-time. Video and voice calls consume high bandwidth, so service providers wish to detect and mitigate them to protect their resources.

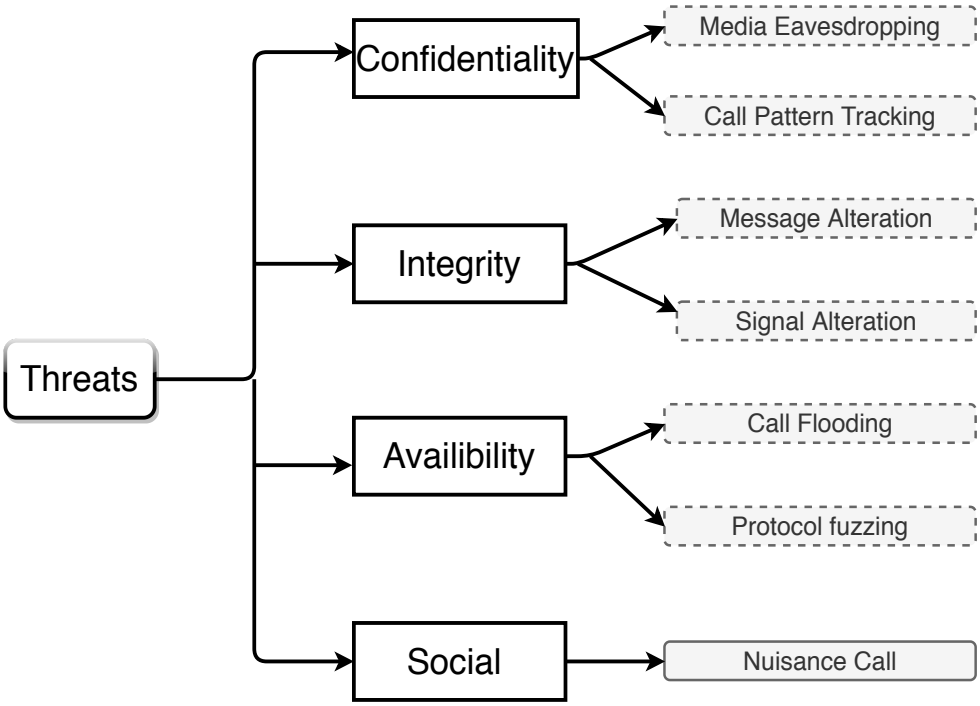


Figure 1. Taxonomy of Internet Telephony Threats.

Several researchers recently addressed voice spam detection over VoIP systems [5–10], but all these solutions are only relevant for automatically dialed prerecorded voice-spam. They cannot distinguish different kinds of undesirable nuisance calls, for example, silent calls generated for Distributed Denial of Service (DDoS) attacks, or live telemarketing calls made for advertisement and scam purposes. Behavioral-based mechanisms [11–15] are the most effective in identifying spammers, but they generate a high false-negative rate as certain legitimate callers are falsely detected as spammers. Besides, all these solutions are subject to whitewashing attacks, as they assume that a spammer will spend a considerable duration in the network without changing its identity. Unless service providers introduce adequate mechanisms to combat different types of nuisance calls generated over their networks, consumers will continue to suffer. Three important criteria must be met by an effective solution to combat nuisance calls over the web. Firstly, the mechanism introduced should not have any observable delay during the call setup. Secondly, the mechanism should completely avoid blocking legitimate calls. Thirdly, the mechanism should be secure from different adversary threats such as whitewashing attacks.

In this paper, we provide a reputation model to detect malicious callers in the network that generate nuisance calls. The paper includes three major contributions. Firstly, a descriptive model for nuisance calls is presented that details the types and characteristics of nuisance calls. It further presents the attributes and behavior of callers who generate nuisance calls. Secondly, a reputation model is presented to detect various kinds of nuisance calls. The model consists of a feature module, recommendation module, reputation evaluation, status module, and decision module. The components are used to compute the

reputation of each caller which is used to differentiate between legitimate and nuisance calls. Lastly, a set of experiments are conducted to study and analyze the performance of our proposed solution in Internet Telephony.

In the rest of the paper, Section 2 summarizes the related work, and Section 3 describes the nuisance call, detection model. Section 4 presents the reputation model and its components. In Section 5, tests demonstrate the feasibility and robustness of the proposed system. Finally, we conclude the paper in Section 6.

2. Related Work

There are two kinds of spam prevalent over the Internet, email and voice spam. Voice spam remains more disruptive and difficult to be detected than email spam due to several reasons. Firstly, email spam can be stored and processed for spam detection while a voice call needs to be processed in real-time. Secondly, email contents are available inside the email body whereas, in calls, contents are only available after the call is established. Thirdly, voice spam consumes high bandwidth, thus may cause congestion in network traffic. Various techniques have been proposed in the literature to detect and mitigate voice spam. The approaches can be broadly categorized into content-based, challenge-based, list-based, trust-based, and statistics-based. The details of each approach are presented as follows:

Content-based: In a content-based approach the conversation is processed in real-time to detect if the call received is spam or not. In [16], a speech recognition system is developed to compare the content of the call with different speech messages. A set of rules are defined to decide whether the content consists of spam or not. Whereas, spectral features are extracted in [17] to create an audio fingerprint. Voice spam is detected by computing the similarity between the fingerprint and the content of the call. However, the content-based approach has several limitations which makes it impractical for Internet telephony applications. Firstly, the speech recognition technology causes observable delays in the call due to its complex processing system. Secondly, the decision of whether a call is a spam or not is taken after the call is received, in which case the spammer has already annoyed the callee. Thirdly, most of the subscribers do not allow their service providers to analyze their call content. Lastly, the spammers can always mitigate speech detection by modifying their content and adding noise.

Challenge-based: In a challenge-based approach, an automatic challenge is created for callers. A caller needs to solve the challenge correctly to proceed with a call. These systems differential a human-generated call from an automated call. Spammers usually use auto-dialers to send pre-recorded spam calls. The challenge-response systems create tests that humans can solve easily but are very difficult for machines to solve. In communication systems voice-based CAPTCHA systems are the most popular as they require users to speak their responses instead of typing them [18]. In [19], a Turing test is introduced that monitors the overlaps in a speech to check whether it is a prerecorded call or not. Whereas, in [20] the researchers combine audio CAPTCHA with a game-theoretic model to authenticate human callers. On the other hand, AutehtiCall [21] is a challenge-response system that requires a caller to prove its identity by using cryptographic keys before each call is sent. Challenge-response systems are effective in detecting recorded spam, however, they have two major limitations. Firstly, these systems introduce a noticeable call setup delay as the challenge needs to be complete before the call can be sent. Secondly, they are only applicable to spam generated by autodialers and are unable to detect human-generated spam calls.

List-based: The list-based approach defines access control that allows calls to be filtered based on the caller's identity. In case of an incoming call, the server extracts the identity of the caller and checks it with the database of managed lists. A decision is made based on the list that the caller belongs to. Usually, the service providers maintain three lists, whitelist, blacklist, and greylist. A whitelist consists of legitimate callers and a blacklist consist of spammers. Whereas, a greylist is maintained for suspicious callers. A

list-based approach causes minimum delay to the call connection process and is fairly easy to implement. However, there are some drawbacks to this approach as well. For instance, it is difficult for legitimate callers to use the services with the same identity if they are falsely blacklisted. On the other hand, if spammers are blacklisted they can easily reenter the network with a new identity and continue with their malicious activities. Furthermore, a list-based approach is always implemented along with another approach to decide which caller is placed in which list. For instance, PSPIT [22] is an example that uses k-nearest neighbor classification to maintain a blacklist of spammers in the network. Whereas in SPIT-AL [23], a web of trust network is used to build a whitelist and blacklist of callers.

Trust-based: In a trust-based approach a trust score is computed for each caller that is used to differentiate a spammer from a legitimate caller. The trust relationship of a caller with each participant is aggregated to determine the global behavior of the caller towards its participants. In a trust-based approach, the social network of the caller can be used to build its global reputation. Models are then used to traverse the network and determine trust between members of the network. For instance, CallRank [24] uses call duration to establish social linkage between callers. Eigen-trust algorithm is then used to determine the local and global reputation of callers using their social linkage. SymRank [15], on the other hand, uses in-degree and out-degree levels to rank callers in the network. In [25], a social network graph is build based on the call data records which is then used to compute the global reputation of each caller in the network. However, these methods may suffer from lengthy delays due to the long reputation search paths in large communication networks. On the other hand, recommendations or referrals can also be used to compute trust scores. For instance, in [26,27], architectures are proposed to accumulate referrals from other participants. The trust values of callers are computed based on the feedback of caller communicating participants. The accumulated feedback score is used to detect and filter spam calls in the network. However, recommendation systems require adequate mechanisms to combat false recommendations and collusive group formation that can use by adversaries to avoid their detection.

Statistics-based: Statistic-based approaches are used to monitor the behavior of callers in the network. The characteristics of calls are extracted such as call rate, call duration, and call frequency. These characteristics provide valid information that can be used to detect the presence of spammers in the network. For instance, the call duration of a spam call is usually very low whereas the frequency of calls made by a spammer in a short duration is very high. Researchers in [11,13] use call duration to differentiate between legitimate caller and spammer. Whereas, call frequency is used by [14] to develop a progressive multi-grey leveling system known as PMG. In PMG, the call rate of each caller is used to determine two levels a short term and a long term grey level. If the summation of the two levels is greater than a pre-defined threshold, the caller is regarded as a spammer. Researchers in [12] combine a different set of features such as frequency of calls, call duration, and the number of outgoing partners of a caller. Whereas in DEVS [28] caller recipient rate, call duration, call traffic, and call rejection rate is used to compute the SPIT Level. The SPIT level is used to determine the state of the caller. Based on the state of the caller incoming call is blocked or send. The statistics-based techniques are effective in detecting spam calls but they also generate high false positives which result in many legitimate calls being detected and blocked as spam calls. Moreover, spammers may adopt the call statistics of the legitimate caller to avoid their detection. Machine learning techniques have also been applied to calling behavior to differentiate between the spammer and legitimate caller. A semi-supervised clustering is used on call parameters to mark each call as spam or legitimate [29]. Whereas, [30] compares ten machine learning methods to classify callers into legitimate and spammers. However, machine learning requires supervised training data and high processing.

Each type of technique used to detect voice spam has its advantage and drawback. We further identify three major limitations in the existing voice-spam detection mechanisms.

Accordingly, we need a new approach to model and detect nuisance calls that overcome these limitations. The three limitations are discussed as follows:

i. Existing techniques are only applicable to automatically dialed prerecorded voice-spam. These mechanisms do not consider other types of unwanted nuisance calls. However, the nuisance calls statistical report presented in [31] shows that live and silent spam calls occur in a much larger quantity compared to recorded spam calls. Figure 2 shows that in 2019 alone the percentage of live and silent calls was 31% and 36%, well above the 14% of recorded calls. Live calls are generally made for telemarketing and scam purposes whereas silent calls occur in Denial-Of-Service (DoS) attacks. Accordingly, the existing spam detection mechanisms do not treat the majority of nuisance calls and need to be revised to detect other more relevant types of spam calls. Moreover, live and silent spam calls are considered to be more harmful to the users as well as to the network.

ii. Several existing mechanisms are very effective in detecting spam in communication networks. They usually correctly identify spammers by using their behavioral statistics. The very high rate of detecting spammer is however coupled with a tendency to a high false-positive rate. This means that many legitimate calls are incorrectly identified as spam. For instance, calls made from legitimate call center representatives have short call duration, high outgoing call rate, and low incoming call rate. These are features very similar to spammers, and thus such calls are prone to be mistakenly identified as spam in the communication network. The reputation damage for a service provider that blocks a legitimate call by misidentifying it as spam is very high. Therefore, we need a new approach that can differentiate with certainty between spammers and legitimate users that have similar call patterns.

iii. The user identity over Internet Telephony is easily generated by filling in self-asserted profile information without any identity proofing. Attackers can easily create fake identities and generate calls without fear of getting penalized. Upon detection, they can perform a whitewashing attack by simply re-entering the network by creating a new identity. Thus, whitewashing remains an effective method for spammers to avoid detection and continue spamming in the network. As per our knowledge, none of the existing methods provide a solution to combat whitewashing attacks. To effectively detect nuisance calls in Internet Telephony it is essential to provide defense against whitewashing attacks.

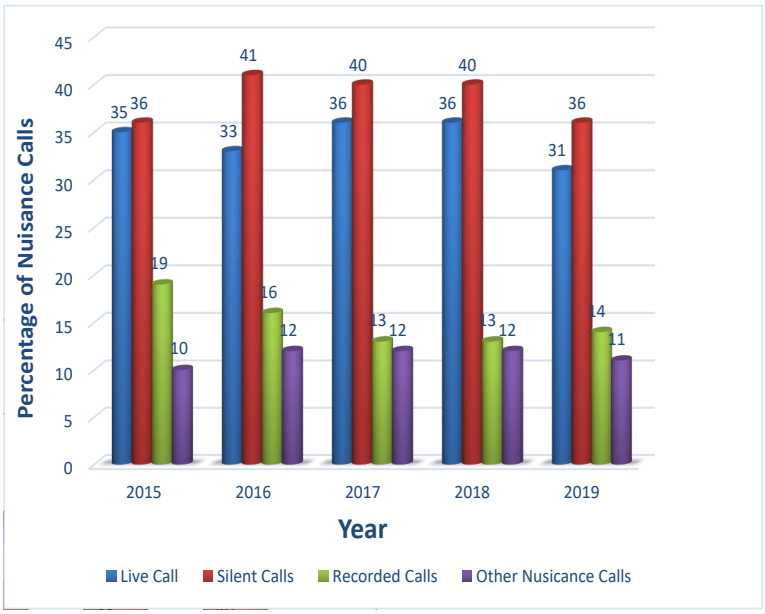


Figure 2. Statistics of users receiving spam calls [31].

3. Nuisance Call

Nuisance calls are considered pollution for Internet Telephony. To effectively detect and combat nuisance calls, it is essential to first examine and understand them. In this section, we present a model to describe nuisance calls over Internet telephony. The nuisance call model is presented in Figure 3. The model incorporates three aspects of nuisance calls (i) purpose, (ii) types, and (iii) attributes. We describe the nuisance call model by discussing the classification and characteristic of nuisance calls in Sections 3.1 and 3.2.

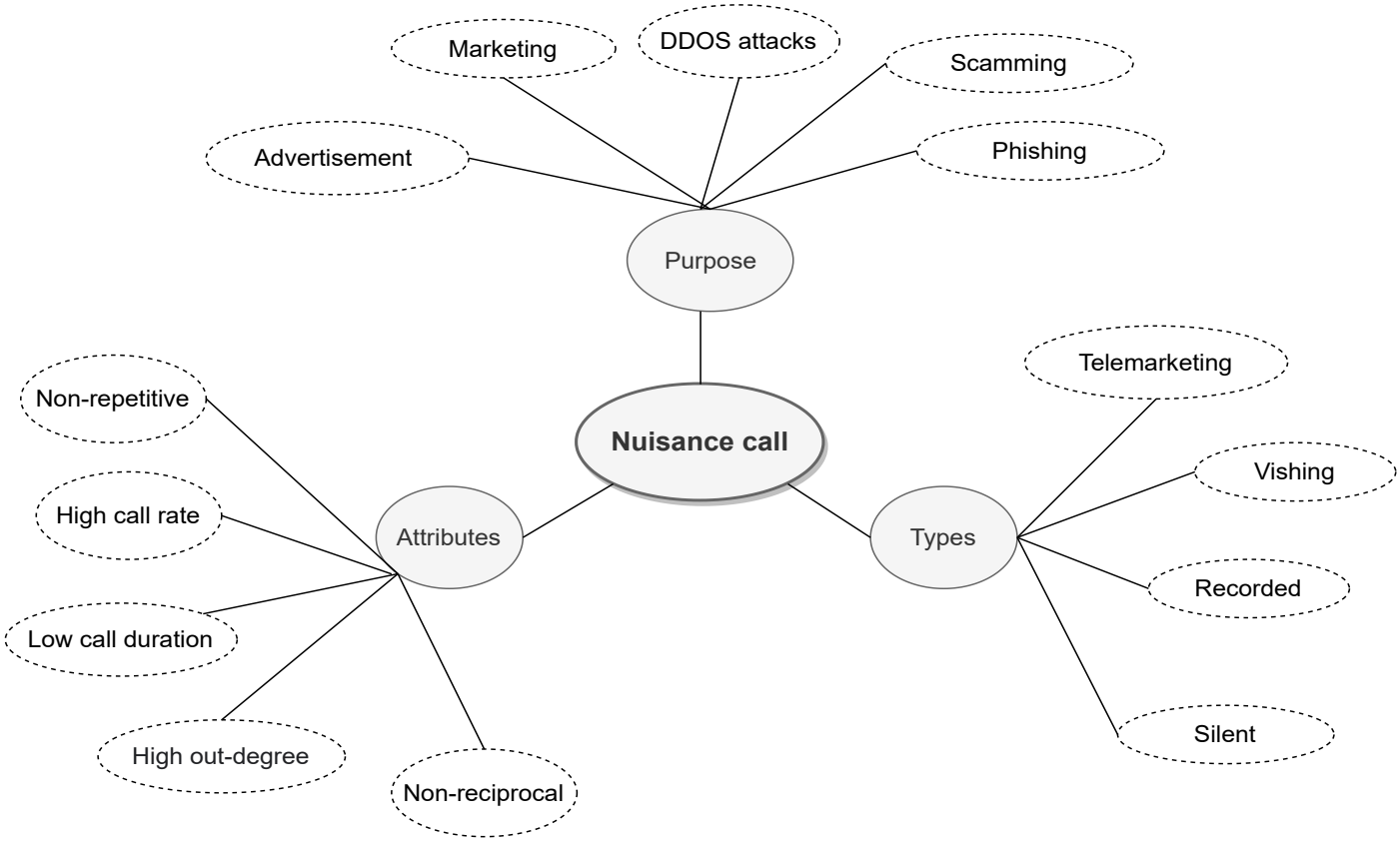


Figure 3. Descriptive model for nuisance call.

3.1. Classification

Nuisance calls can be described as unsolicited spam calls generated over a communication network. Nuisance calls use Internet infrastructure to instantiate unsolicited messages to target groups of users. Nuisance calls are generated for many reasons including, advertisement, marketing, scamming, phishing, and attacks on the network as shown in Figure 3. Nuisance calls remain highly disruptive. They are usually inconvenient and annoying but for more vulnerable consumers they can also cause real harm. Nuisance calls take many forms and come in different shapes and sizes. Nuisance calls can be broadly characterized into four types including telemarketing and vishing, silent and recorded calls. Telemarketing and vishing calls are manually generated, whereas silent and recorded calls are automatically dialed using autodialers. The description and purpose of each category are provided below:

1. Telemarketing: Telemarketing calls are made by salespersons to convince customers in buying their products or services. It is a method of direct marketing that involves direct human interaction. Telemarketing is looked upon negatively by consumers as they consider them annoying and disturbing in nature. Telemarketers often use high-pressure techniques to sell their products which are considered unethical. Furthermore, they may consist of several scams and frauds in which fraudulent telemar-

keters try to deceit and cheat their victims. Phone scams often involve some sort of payment from victims by fooling them. Telemarketing is usually beneficial for mobile cellular networks as they earn more revenue when telemarketers generated calls over the network. However, Internet telephony operates on a different business model in which their focus is to retain their customers by facilitating them with enhanced services. Therefore, Internet telephony services put their utmost effort to reduce telemarketing over their network.

2. Voice phishing: Vishing or voice phishing is conducted over a phone call in which the attacker tricks a callee into providing confidential information that is later misused. The attacker uses social engineering to trick the victim into sharing personal or financial details such as account number, card number, and passwords. The attacker usually claims to be from some trusted organization such as a bank or telephone company. By claiming to be from a legitimate organization they deceive the victim into thinking that providing the information is for their benefit. Attackers may also deceive the victim by tricking them to install malware on the phone that tracks and extracts information about the victim.
3. Recorded: Recorded calls are automatically dialed calls that are broadcast over the communication network for marketing and advisement purposes. Such calls are sent in bulk and have a fixed duration of the call. Instead of dialing each number separately the recorded call are sent repeatedly using autodialers. An autodialer is a software that automatically dials telephone numbers and plays a recorded message when the call is received. Internet telephony remains an attractive medium to play recorded messages due to its cost-effectiveness. Telemarketers usually use recorded advertisements and messages to promote their products and services to a large number of audience promptly.
4. Silent: Silent calls are abandoned calls in which the callee hears nothing. Silent calls are also generated using autodialers where instead of playing a recorded message the callee hears nothing and has no means to determine who the caller is. The silent calls are usually generated purposely to conduct DDoS attacks over the network. The purpose of a DDoS attack is to prevent callers from using the network. An attacker or a group of attackers use many autodialers to generate an immense amount of silent calls over the network at the same time. A flood of silent calls can halt or significantly disrupt the services of the network. These types of nuisance calls if generated in bulk are highly disruptive for the Internet telephony providers. It harms the reputation of the service provider as the consumers are either unable to access the network or are unable to receive the expected quality of service.

3.2. Characteristics

The subscribers of Internet Telephony can be classified into legitimate and malicious callers. Legitimate callers are subscribers of Internet telephony that use services in a permissible manner. On the contrary, malicious callers are spammers that generate nuisance calls. Nuisance calls are generated for marketing, advertising, scamming, phishing, and DDoS attacks as discussed in Section 3.1. Therefore, their calling behavior is distinguishable from legitimate callers. We discuss several attributes of spammers based on their calling behavior. Call frequency is the number of calls made by a caller in a specific time period. Spammers launch a large number of calls continuously during a certain time period, hence their call frequency remains very high. In every call, the spammer attempts to targets a new callee. Thus, their calling behavior is non-repetitive in nature. On the other hand, legitimate callers usually have a moderate call frequency where their calls have a repetitive pattern within their social network. The call frequency and repetitive nature of calls can help distinguish a spammer from a legitimate one. But if used alone they may result in some legitimate calls being detected as nuisance calls as some legitimate callers might have a high call frequency and non-repetitive behavior at certain times. For example, a university sending important updates to their students may have non-repetitive and

high call frequency. The call duration between two participants is the total talk time of all calls placed between them. Spammers can be categorized with a high number of low call duration with their communicating participants. This behavior of spammers is because of several reasons. Firstly, spammers do not call a callee repeatedly. Secondly, due to the content of their calls most callees would hang up immediately after learning the nature of the call. Thirdly, spammers rarely receive calls from legitimate callers. This results from spammers having a large number of low call duration calls. This feature can be used to differentiate spammers from socially connected legitimate callers who have considerable call duration within their social network. The in-degree of a user is the number of unique callers calling this user whereas the out-degree of a user is the number of unique callees this user calls to. A spammer usually calls a large number of unique callees and receives a response from few callees. Therefore, spammers usually end up with an unbalanced disproportionate in/out-degree, with high outgoing calls and low incoming calls. Legitimate callers usually have bi-directional interactive communications with other users, like a reciprocal call behavior towards their friends and family members, and thus a balanced in/out-degree.

4. Caller Reputation Model

In this section, we propose a reputation model that computes caller reputation to detect nuisance calls in Internet Telephony. The solution is developed based on different requirements that are extracted from the limitations of existing methods presented in Section 2. The requirements are as follows:

- *Requirement 1:* The nuisance detection mechanism should be implemented in such a way that minimum changes are required to the infrastructure of the web service provider.
- *Requirement 2:* The nuisance detection mechanism should work in parallel with the signaling process, to cause minimum observable delay to the caller.
- *Requirement 3:* The nuisance detection mechanism should be able to detect nuisance calls while eradicating the possibility of falsely detecting a legitimate call as a nuisance call (false positive).
- *Requirement 4:* The nuisance detection mechanism should be able to detect different types of nuisance calls generated over Internet telephony, covering the cases discussed in Section 3.1.
- *Requirement 5:* The nuisance detection mechanism should be robust against whitewashing attacks which are used by malicious callers to discard their bad reputation in the network.
- *Requirement 6:* The nuisance detection mechanism should allow the user to choose what action the service provider should take in case a malicious caller tries to send a call request.

Based on these requirements we built a reputation model to detect nuisance calls. The functional architecture of the model is presented in Figure 4. The reputation model consists of five components namely, Features Module, Recommendation System, Reputation Computation, Status Module, and Decision Module. When a caller initiates a call, the signaling function is executed to route the call to the callee. In parallel to the signaling function, the caller reputation value and status are extracted from the reputation module and status module respectively. The reputation value is used to determine whether the call being initiated is legitimate or malicious. The decision module decides to reject or send the call based on the reputation value of the caller and the preferences set by the callee. The reputation value is computed based on the call features extracted by the feature module and recommendations provided by the recommendation system. The details of each component are described in the following subsections:

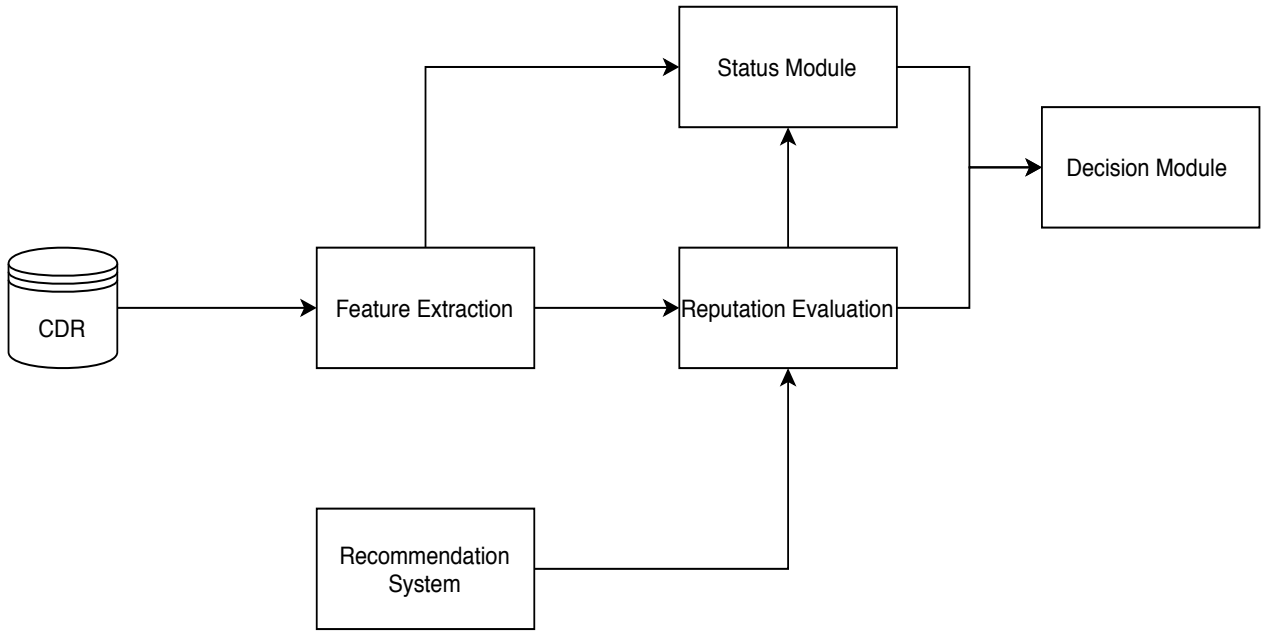


Figure 4. Reputation model to detect nuisance calls.

4.1. Feature Module

The call feature module uses the call data records to extract the required features necessary to compute the reputation of any caller. The call data records for each user are stored by the Internet Telephony service provider. A record includes caller identity, callee identity, and timestamps for call initiation/termination. The timestamps are used to compute the talk time between two users, and the talk time can be an indicator of the amount of trust between the two users. A strong trust relationship can indicate whether two users have high talk time and vice versa. To extract the relevant and most recent calling behavior of the caller we apply the sliding window concept. As shown in Figure 5, we consider time windows T consisting of n time units t measured form an initial time t_0. A new time window of the same length is created by adding a new time unit and removing the oldest time unit, thus "sliding" by one unit. T_k is the time window after k slides, where $k > 1$. This allows the most recent behavior of the caller to be captured. The time unit is only considered if there is call activity present in it. The size and number of time units can be set differently by each service provider based on their policy. For instance, if a service provider selects 5 time units of 4 min each this will make the time window 20 min.

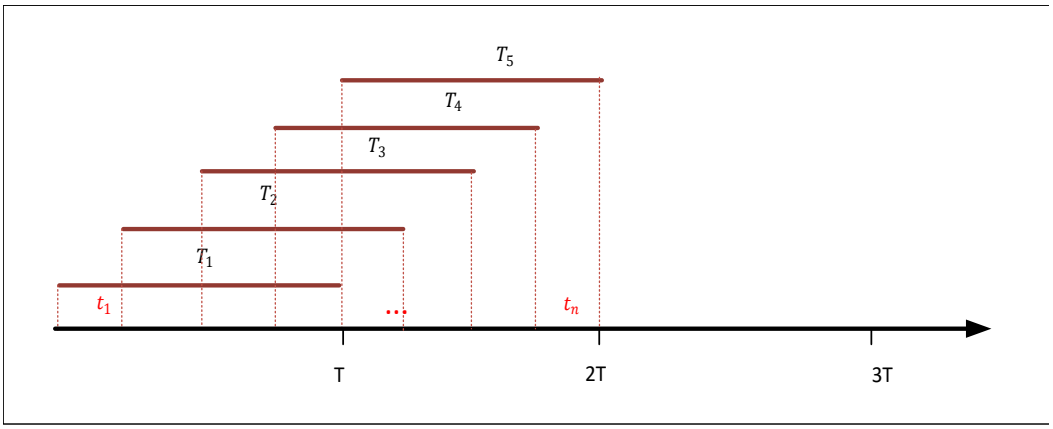


Figure 5. Sliding Time Window Principle.

The ego network for a particular ego node consists of all nodes to whom the ego is directly connected to. The call feature module uses call data records to create an *ego network* of each user in the network in a particular time window. This user-specific ego network consists of a user and the entire set of peers to whom it is connected. The ego network is used to compute the *Total Talk Time (3T)* between two peers which is the sum of the duration of all calls made between them. An example of an ego network for communication scenario is shown in Figure 6. In this scenario, the user is connected to four other communicating participants called peer 1, 2, 3, and 4 in a particular time window. The user has a reciprocal call behavior with peer 1 and peer 3 as calls are placed in both directions. It only has a repetitive behavior with peer 3 as three calls are placed by the user. The figure further shows that the user is connected to peer 4 and peer 2 as it sends a call to peer 4 and receives a call from peer 2. The ego network is used to compute $3T$ for a user with each of its communicating participants. The maximum value of the $3T$ depends upon the time window selected. In the example the time window is 20 min therefore the maximum value of $3T$ will be 20. The $3T$ with peer 1, peer 2, peer 3, and peer 4 are 3.2, 0.3, 0.5, and 11.6 respectively. From the figure, it can be observed that the user has repetitive and reciprocal behavior with peer 3. Thus, the value of $3T$ incorporates the reciprocal and repetitive nature of calls placed between them. The higher reciprocal and repetitive behavior is reflected by a higher value of $3T$. A high $3T$ value between two peers can indicate a high trust relationship. Additionally, the call feature module computes also the *out-degree* of each user, as the number of peers to whom the user has placed the call. In the ego network of Figure 6, the user out-degree is 3, as the user has called peer 1, 3, and 4. A high out-degree together with a short $3T$ indicates that the caller is not very popular among the network and is most likely spamming in the network.

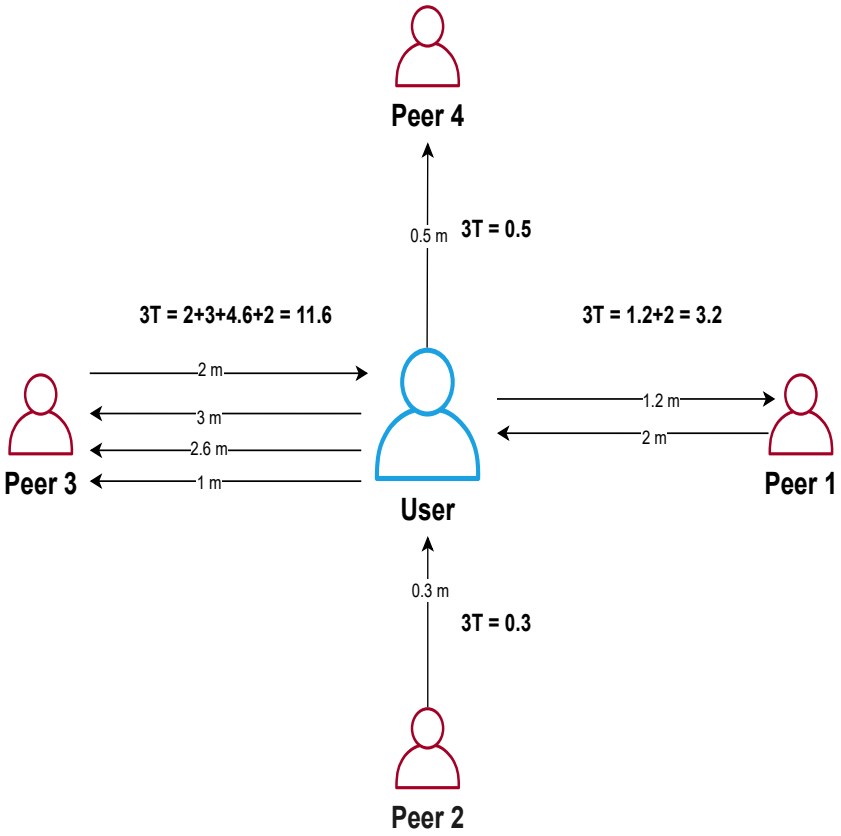


Figure 6. Caller neighbourhood in communication network.

4.2. Recommendation System

The recommendation module collects recommendations about each network user. Any user u_j can recommend malicious behavior of its caller p_i as follows:

$$Rec_{u_j \rightarrow p_i} = \begin{cases} -1 & \textit{if malicious} \\ 1 & \textit{otherwise.} \end{cases} \tag{1}$$

To combat false recommendations in the network, three recommendation criteria are followed. Firstly, a recommendation can only be provided after a call session is terminated. Secondly, only the callee receiving the call can recommend the caller who placed the call. Thirdly, a callee can only recommend a caller once. These criteria are used to collect recommendations about the user in the network. However, not every recommendation can be considered trustworthy. Therefore, the credibility parameter of a user is used to compute the trustworthiness of a callee providing a recommendation. The credibility of a user is evaluated within the specified period as follows:

$$Cr(p_j) \epsilon [0, 1] \tag{2}$$

Credibility indicates the sincerity of a peer in giving correct recommendations. To determine the credibility of a caller in the network we use the honesty parameter defined in [32]. The honesty metric represents the likelihood that a communicating peer provides correct recommendations. This is determined by evaluating the degree to which the recommendations given by the peers are different from what the reputation indicates. For instance, if a peer recommends a caller as legitimate and the reputation of the caller also indicates the same then the recommendation is considered as honest. Otherwise, the recommendation is considered dishonest. The honesty parameter for a peer is simply computed as the number of honest ratings divided by the total number of ratings.

4.3. Reputation Evaluation

The reputation module computes the reputation of each caller as a numeric value. The reputation $Rep^{T_i}(u_i)$ of the caller u_i for time window T_i is presented as follows:

$$Rep^{T_i}(u_i) = \frac{\sum_{j=1}^{n} 3T_{p_j} \times Rec_{p_j \rightarrow u_i} \times Cr^{T_{i-1}}(p_j)}{OD_{u_i}}, \tag{3}$$

where n are the total number of peers user u_i is connected to and OD_{u_i} is the out-degree of caller u_i. $3T_{p_j}$ is the Total Talk Time between user u_i and peer p_j. A strong trust relationship is represented by a high $3T$ value whereas a weak trust relationship is represented by low $3T$ value. The $3T_{p_j}$ is weighted with the credibility of each peer, represented by $Cr(p_j)$. Thus, the user's reputation is high if it manages to have good $3T$ with its peers whereas its reputation decreases if it has a small $3T$ with a large number of callees. The range of $Rep^{T_i}(u_i)$ depends upon the value of time window. If the time window is set to be 10 min then the value of $Rep^{T_i}(u_i)$ will be in the range of 0–10. To address the dynamic behavior of spammers, short-term and long-term reputations are computed. A large time window is used to compute long term reputation $Rep^{T_i^L}(u_i)$ whereas a short time window is used to compute short-term reputation $Rep^{T_i^S}(u_i)$. The smaller time window reflects the caller's most recent behavior. $Rep^{T_i^S}(u_i)$ will be used if the difference between short-term and long-term reputation is less than a certain threshold. This indicates that the peer has recently started behaving maliciously:

$$Rep(u_i) = \begin{cases} Rep^{T_i^S}(u_i) & \textit{if } Rep^{T_i^L}(u_i) - Rep^{T_i^S}(u_i) > \textit{threshold} \\ Rep^{T_i^L}(u_i) & \textit{otherwise.} \end{cases} \tag{4}$$

The short-term and long-term reputation is used to detect the behavior of spammers quickly. The overall reputation of the caller cannot quickly increase by a small number of good call transactions, that is, the reputation is relatively stable for good behaviors. However, the reputation will quickly drop if the caller starts acting maliciously in the network.

4.4. Status Module

The status module is used to deter whitewashing attacks. Users of Internet Telephony perform whitewashing to shed their bad reputation by re-entering the network with a new identity. In our system, nuisance calls can only be realized by achieving a respectable reputation in the network, so that they are allowed to communicate freely. For a user to communicate freely it requires time to gain a respectable reputation level. A user who changes identity will not be able to generate nuisance calls without first building a respectable reputation in the network, which takes time and effort. Therefore, this approach removes the advantage that whitewashing attacks can provide to an attacker. The status module categorizes users of Internet Telephony into *Beginners* and *Mature* users. *Beginners* are newcomers that recently entered the network. They are allotted a limited quota of calls. Because our system allows *Beginners* to communicate with limited unique callees and place a certain amount of calls in a time period, *Beginners* are not able to generate nuisance calls in the network. On the other hand, *Mature* users are allowed to communicate freely without any restrictions. Therefore, for each call request placed by *Mature* users, their reputation is checked to determine whether this is likely to be a nuisance or legitimate call. To become a *Mature* user, an *Beginner* user has to pay a fee in the form of building first a good reputation. This is the social cost incurred to *Beginners* to communicate freely in the network. Thus, the status module can deter whitewashing attacks conducted by malicious users to continuously generate nuisance calls in the network.

4.5. Decision Module

The decision module is responsible for processing all call requests. It extracts information from different modules and determines whether a call is legitimate or a nuisance. The flow diagram of the decision module is shown in Figure 7. When a call request is received, the decision module extracts the caller and callee identity from the call request. Then it checks the status of the caller from the status module. If the caller is a *Beginner* it examines the call quota of the caller. If it is within the quota, the call request is sent to the callee. If the *Beginner* has already consumed its quota the call request is rejected. If it is a *Mature* user the reputation module is used to extract the reputation of the user. Using a certain threshold set by the service provider the incoming call is categorized into legitimate and nuisance call as follows:

$$Call\ Type = \begin{cases} Nuisance & if\ Rep(u_i) < Threshold \\ Legitimate & otherwise. \end{cases} \tag{5}$$

Call requests categorized as legitimate are sent to the callee. Otherwise, for calls categorized as a nuisance call the preference of the callee is checked to process the call, resulting in one of the following actions (i) Call is sent with a warning of being a nuisance call, (ii) Call is sent to voice recorder of the callee, (iii) Call is rejected, (iv) A notification about a call is sent to the callee.

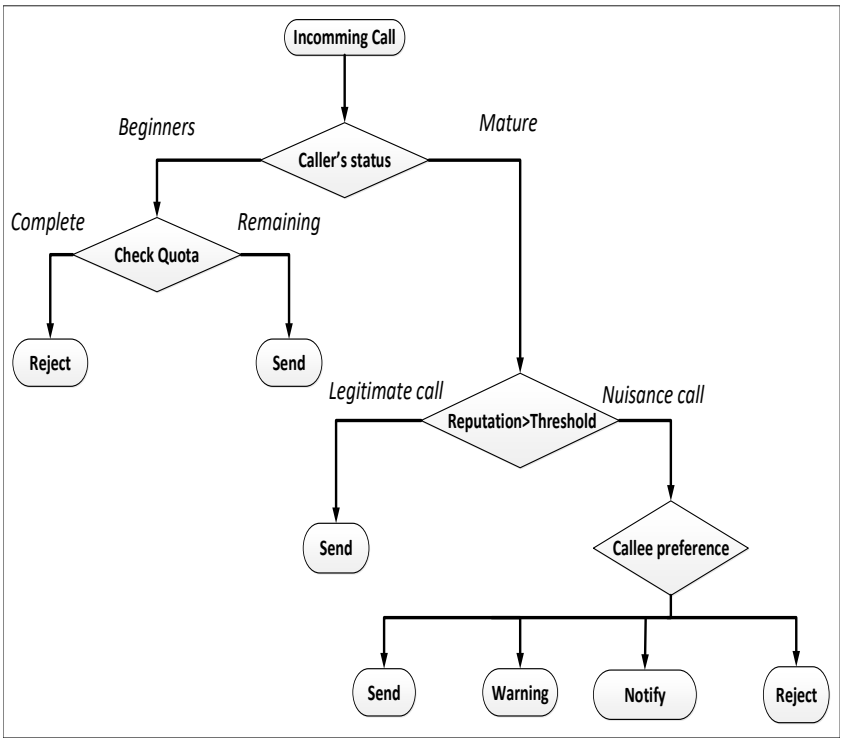


Figure 7. Decision module flow diagram.

5. Experimentation and Results

To evaluate the performance of our proposed solution, we first describe the simulation setup and various types of callers present in the network. A synthetic call data record is used to generate a communication network to perform our experiments. The evaluated performance and efficiency of our solution are then presented. Performance is computed in terms of accurately detecting nuisance and legitimate calls under various conditions. We further compared the performance of our solution with analogous threshold-based spam detection techniques.

5.1. Simulation Setup

We generated a synthetic call data record to conduct various experiments. The experiments are conducted in Matlab. We use the structural properties [33] of telecom call graphs and call statistics [34] to generate the synthetic call record. Our simulated network follows a power-law degree distribution with power law degree exponent selected to be between $2 < gama < 3$. Therefore, the majority of the callers in the network have few peers and only minorities have a large number of peers. We use 5 time units for the time window, and the sliding window technique. We use the configuration data from [25,35] to simulate callers in the network. The network includes both legitimate and malicious callers. Legitimate callers are classified into (i) genuine and (ii) distinct callers, whereas malicious callers are further classified into (i) telemarketers, (ii) autodialers and (iii) attackers. We simulate a communication network of $n = 300$ callers having 10% live telemarketers, 10% autodialer, 10% attackers, 60% genuine callers and 10% distinct callers in the network, with the call rate distribution and call duration parameters summarized in Table 1. We describe each type of caller as follows:

1. Genuine: Genuine callers are legitimate users of the network, characterized by long-duration repetitive and reciprocal calling behavior with their social group. We use the statistics presented in [15] to model genuine callers in our network. The call rate of genuine callers follows a Poisson distribution with mean 5 calls. 80% of their calls are distributed within the social group which consists of 4–5 peers. The call duration of genuine callers is modeled using a normal distribution with mean 5 and variance 3.

2. Distinct: Distinct callers are legitimate users of the network that have high out-degree and short duration calls with a very low amount of repetitive and reciprocal calls. For instance, an employer that delivers short messages to its employees or a job seeker that calls different organizations to apply. Therefore it is difficult to differentiate them from malicious callers. For the distinct caller, we use a Poisson distribution for call rate and exponential distribution for call duration.
3. Telemarketers: Telemarketers are malicious callers that follow a non-repetitive and non-reciprocal call pattern with a high out-degree when compared to genuine legitimate callers in the network. A telemarketer tries to connect with a large number of peers while receiving a small number of calls. We choose a constant value for the call rate because Telemarketers generate calls repeatedly in a fixed time unit. The calls made by Telemarketers usually are of short duration due to the nature of their calls. Therefore the call duration is generated similar to a distinct caller using the same distribution and mean value.
4. Autodialers: Autodialers are software that automatically generates pre-recorded advertisements calls. Autodialers usually collect identities by crawling the web or using telephone directories and generate a fixed amount of calls in a time period. Therefore, we choose a constant value for the call rate. Autodialers generate pre-recorded short voice messages, however, callees usually try to end the call right after detecting that it is a prerecorded call. Therefore, the lognormal distribution is a good representation for their call duration, here having $\mu = 0.5$ and $u = 0.3$.
5. Attackers: Attackers are malicious callers that generate silent calls in bulk to conduct a DDoS attack on the network. They usually flood silent calls in the network to consume network resources and overwhelm the service, so that legitimate call requests cannot be processed. As attackers flood silent calls in the network, we chose a constant value for call rate and call duration as shown in Figure 1.

Table 1. Configuration.

Caller Type	Call Rate	Call Duration
Genuine	Poisson $\mu = 3$	Normal $\mu = 5, \sigma = 3$
Distinct	Poisson $\mu = 7$	Exponential $\mu = 5$
Telemarketer	Constant 10	Exponential $\mu = 5$
Autodialer	Normal $\mu = 0.5$ and $u = 0.3$	Exponential $\mu = 2$
Attacker	Constant 50	Constant 0.1

5.2. Performance Evaluation

We perform four experiments to show the performance of our reputation module. We use the following four metrics to compute performance:

- *False Positive Rate:* It is the number of legitimate callers wrongly identified as malicious callers over the total number of legitimate callers in the network.
- *True Positive Rate:* It is the amount of malicious caller correctly identified over the total number of malicious callers present in the network.
- *Detection Accuracy:* It is the number of correct identification of the caller's nature over the total number of callers present in the network. A correct identification occurs when genuine and distinct callers are detected as legitimate, while telemarketers, autodialers, and attackers are detected as malicious.
- *Detection Rate:* It is the percentage of detected nuisance calls over the total number of nuisance calls generated in the network.

5.2.1. Exp 1: Impact of Recommendation

In this experiment, we show how recommendations influence caller reputation, which further helps to identify malicious callers in the network. We use the *True Positive Rate* to show the number of malicious callers correctly identified in the network. This includes

telemarketers, autodialers, and attackers. Correct identification will help the decision module to combat nuisance calls generated in the network. Figure 8 presents *True Positive Rate* for the percentage of callees reporting nuisance calls in the network. It can be observed that the *True Positive Rate* improves with the increased percent of callees reporting nuisance calls. This shows that with a high amount of recommendations there is a better chance to identify malicious callers correctly. This is because recommendations decrease the overall reputation of the malicious caller. The decrease in the reputation of malicious callers allows them to be detected more easily. Moreover, the credibility factor allows false recommendations to be weighted less as compared to trustworthy recommendations. Figure 8 reveals that if at least 30 percent of the callees start recommending in the network, the *True positive rate* goes to 1. This means that service providers need to encourage more callees to report nuisance calls. The service provider may provide incentives to encourage their subscriber to report nuisance calls.

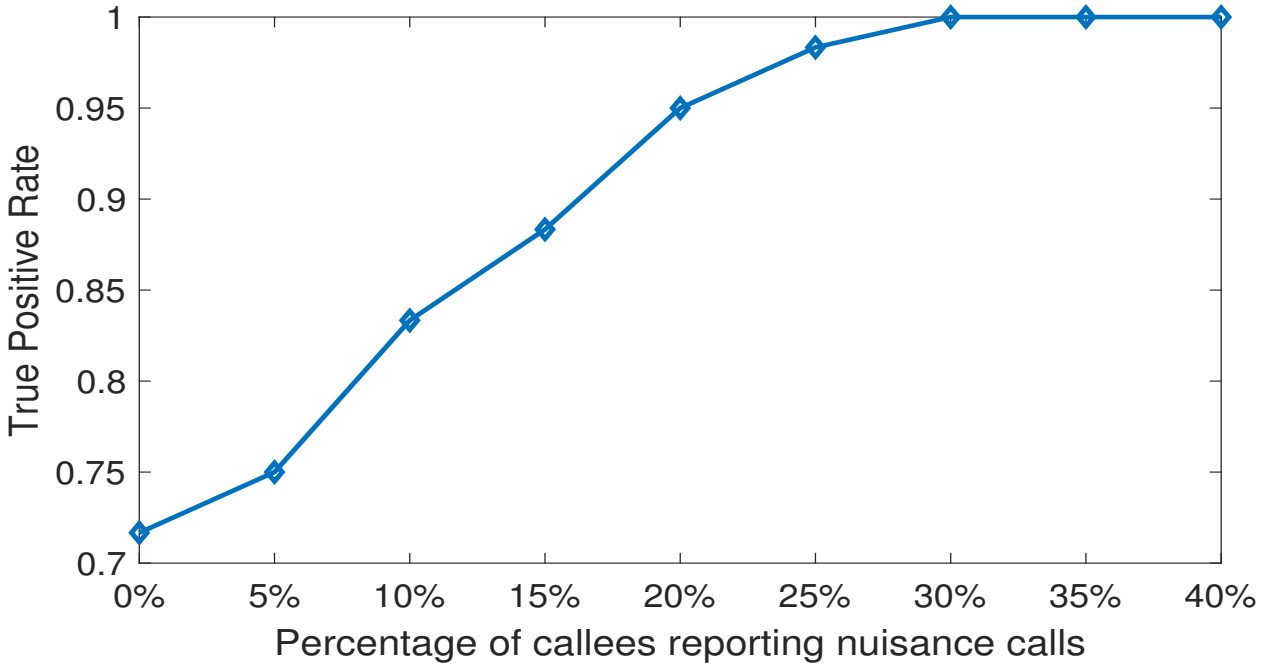


Figure 8. Performance in terms of recommendations.

5.2.2. Exp 2: Computing Detection Accuracy

In this experiment, we compute the *Detection Accuracy* using the caller's reputation. Figure 9 shows the *Detection Accuracy* with 15% of the callees reporting the malicious callers in the network. Initially, callers have a neutral reputation, that builds up as new time windows are created. Legitimate callers gain reputation while malicious callers lose their reputation due to their behavior. Therefore the *Detection Accuracy* increases over time. We can observe from the figure that the *Detection Accuracy* stabilizes to 0.98 after a few time windows. To further investigate the type of callers detected correctly, we computed the *Detection Accuracy* for each type of caller for time window 8. We observed that all the legitimate callers, including genuine and distinct callers, were correctly identified. This means that none of the legitimate calls generated were falsely detected as malicious calls. This is very crucial as blocking legitimate calls decreases the overall reputation of the service provider. Regarding malicious callers, autodialers and attackers were completely detected. However, the telemarketers are detected with an *Detection Accuracy* of 0.98. This means that only a few telemarketing calls will go undetected and will be considered legitimate calls. This shows that caller reputation can effectively detect malicious callers while completely minimizing the chances of falsely detecting a legitimate caller as a malicious caller.

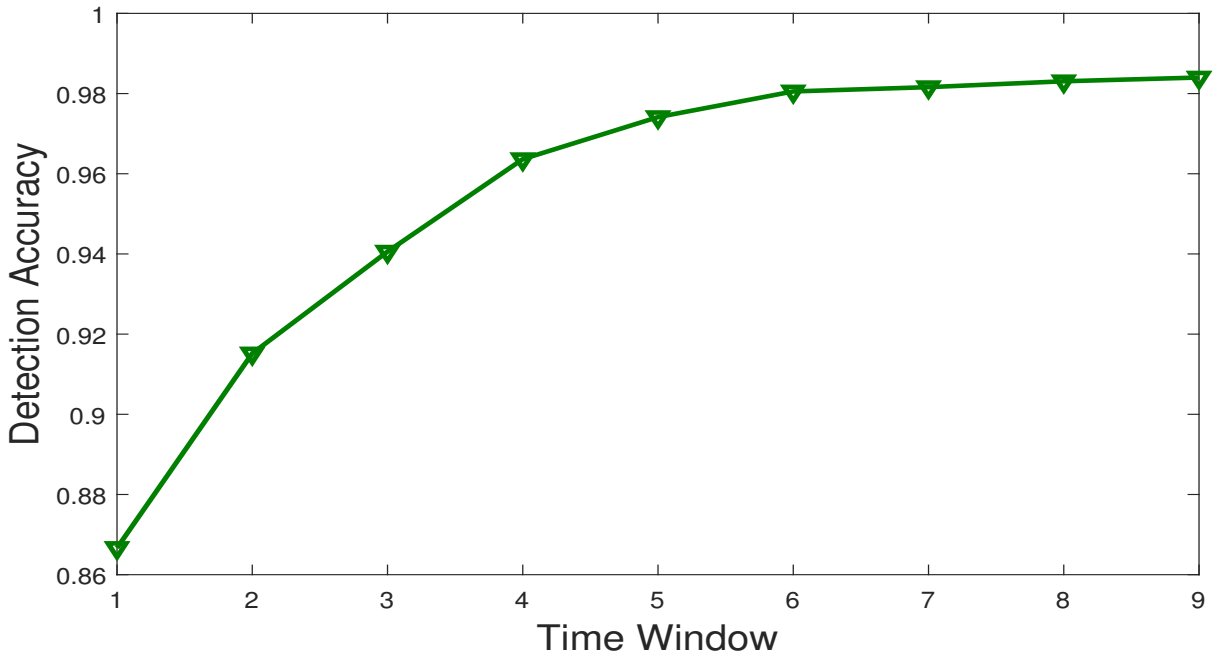


Figure 9. Detection Accuracy.

5.2.3. Exp 3: Efficiency Against Whitewashing Attacks

This experiment shows the effectiveness of the status module to stop whitewashing attacks. The *Detection Rate* is used, representing the percentage of nuisance calls detected in the network. Figure 10 compares the performance of caller reputation used with and without the status module in terms of *Detection Rate*. In this experiment, we consider 50% of the malicious callers performing whitewashing attacks to clear their bad reputation and start afresh to generate nuisance calls. We selected 5%, live telemarketers, 5% autodialers, and 5% attackers that perform whitewashing. The status module can prevent malicious callers from generating nuisance calls when they re-enter the network. Figure 10 shows that when using the status module the *Detection Rate* increases significantly. The status module is effective in acting as a deterrent against whitewashing attacks by removing its advantages. If a malicious caller changes identity it has to earn a respectable reputation again before it can start generating further nuisance calls in the network. Thus, it has to act legitimately in the network for a while. This reduces the number of nuisance calls that are placed, and those that go undetected in the network. Without a status module, a malicious caller may attain a new identity at zero cost. If detected, a malicious caller can re-enter the network under a new identity. With the new identity, the malicious caller would attain a neutral reputation which would allow it to instantly start generating nuisance calls in the network. The nuisance calls generated would go undetected for a long period until the reputation of the caller drops below the threshold. This results in a low detection rate of around 40%. On the other hand, with the status module, the detection rate goes higher to around 80%.

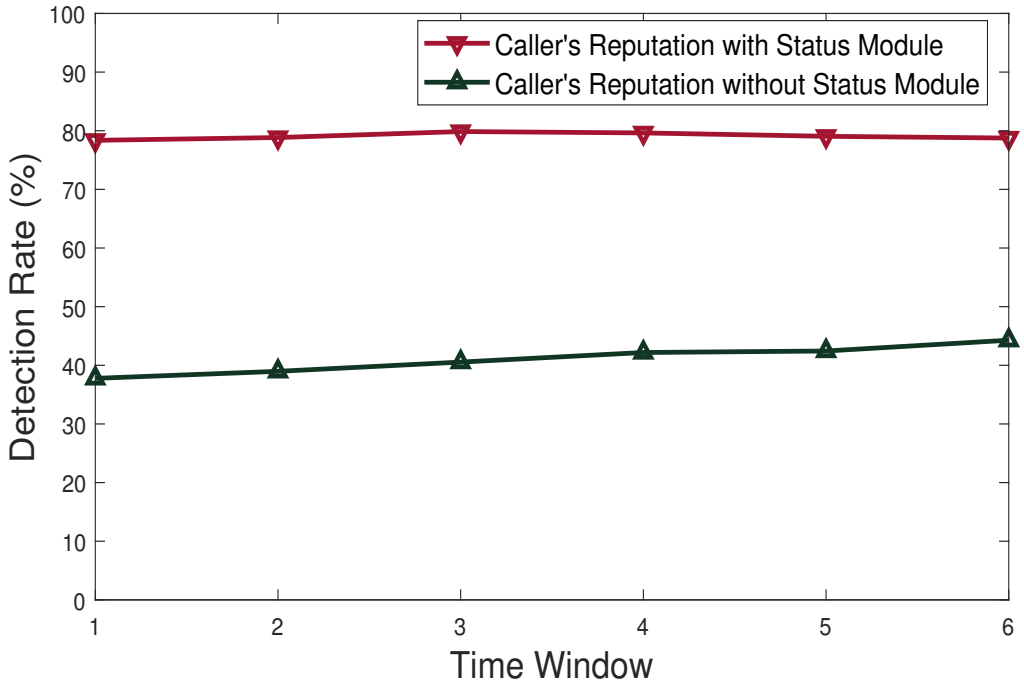
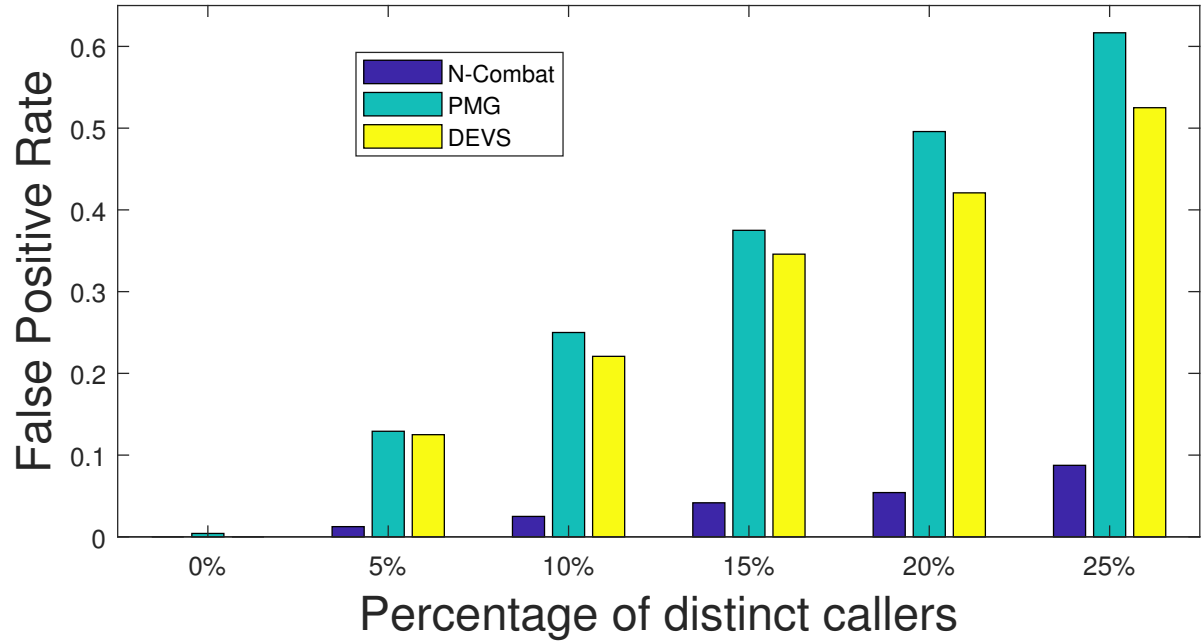


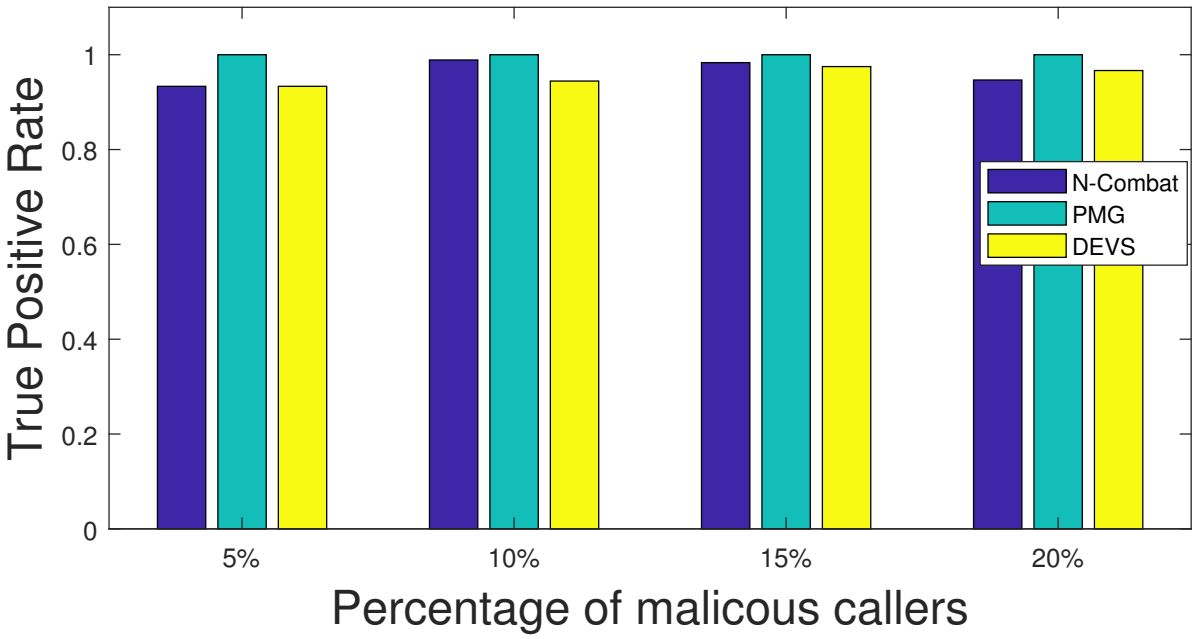
Figure 10. Efficiency against whitewashing.

5.2.4. Exp 4: Performance Comparison with PMG and DEVS

In this experiment, we compare caller reputation with threshold-based voice spam combating techniques. We implemented two of the popular spam detection solutions: PMG and DEVS. Both solutions detect spam based on different call attributes and a pre-defined threshold. PMG determines a grey level for the spammer using call density. If the grey level of a caller reaches a certain threshold, calls made by this caller are blocked. DEVS is largely based on call duration and number of call recipients, using a decision threshold to decide whether a caller is a spam caller or not. For further details on PMG and DEVS implementation please refer to [14,28] respectively. In order to compare the performance, we use *False Negative Rate* and *False Positive Rate* as shown in Figure 11. Figure 11a presents the *False Positive Rate* against the percentage of distinct callers present in the network. Distinct callers are legitimate callers with call patterns similar to spammers, thus are the best candidates for false positives. From Figure 11a it can be observed that caller reputation outperforms PMG and DEVS in terms of false positive rate. Even with 25% distinct callers present in the network, the *False Positive Rate* for caller reputation is below 0.1. On the other hand, PMG and DEVS are unable to detect distinct callers and thus have a high *False Positive Rate*. With 25% distinct callers the *False Positive Rate* is above 0.5. This leads to a high number of legitimate calls falsely detected as nuisance calls which are damaging to the reputation of the service provider. This shows that the existing techniques such as PMG and DEVS do not have any mechanisms to avoid false detection of nuisance calls which is one of the major limitation identified in Section 2. Figure 11b shows the *True Positive Rate* against the percentage of malicious callers present in the network. From the figure, it can be observed that all three solutions have almost the same true positive rate. With 20% malicious caller present in the network, all three have a true positive rate of above 0.9. Thus, we can conclude that caller reputation is a compatible solution in terms of *True Positive Rate* while it performs exceptionally well in terms of *False Positive Rate* when compared to DEVS and PMG.



(**a**)



(**b**)

Figure 11. Performance Comparison in terms of (**a**) False Positive Rate and (**b**) True Positive Rate.

6. Conclusions

In this paper, we present a caller reputation model to detect nuisance calls present over Internet Telephony. The behavior of the caller is assessed by extracting call features from call data records. The call features and recommendations from reliable communicating participants are then used to compute caller reputation. For each incoming call, the reputation of the caller is used to detect whether the call placed is legitimate or a nuisance. A status module is used to combat whitewashing attacks conducted by malicious callers to avoid detection. To the best of our knowledge, this is the first model that protects

communication systems from different types of nuisance calls such as telemarketing, phishing, recorded, and silent calls. The experiments realized prove the effectiveness of our solution, showing that the caller reputation can be used effectively to maximize the detection of nuisance calls while allowing all legitimate calls to pass through the system. As our future work, we intend to develop a software architecture and present workflows to show how the caller reputation model will be used in the normal call setup process.

Author Contributions: Individual contributions of authors are as follows: Conceptualization, I.T.J. and K.T.; methodology, I.T.J.; validation, I.T.J.; review and editing, T.M., N.C.; supervision, N.C.; funding acquisition, F.A. All authors have read and agreed to the published version of the manuscript.

Funding: This work is partly supported with the financial support of the Science Foundation Ireland grant 13/RC/2094_P2 and partly funded from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No 754489.

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

References

1. Jennings, C.; Boström, H.; Bruaroey, J. WebRTC 1.0: Real-Time Communication between Browsers; W3C Recommendation. 26 January 2021. Available online: https://www.w3.org/TR/2021/REC-webrtc-20210126/ (accessed on 26 January 2021).
2. Javed, I.T.; Copeland, R.; Crespi, N.; Emmelmann, M.; Corici, A.; Bouabdallah, A.; Zhang, T.; El Jaouhari, S.; Beierle, F.; Göndör, S.; et al. Cross-domain identity and discovery framework for web calling services. *Ann. Telecommun.* **2017**, *72*, 459–468. [CrossRef]
3. Persistence Market Research. *Global Market Study on VOIP Services*; Technical Report; Persistence Market Research: New York, NY, USA, 2018.
4. Keromytis, A.D. A Comprehensive Survey of Voice over IP Security Research. *IEEE Commun. Surv. Tutor.* **2012**, *14*, 514–537. [CrossRef]
5. Zhang, Y.; Wu, H.; Zhang, J.; Wang, J.; Zou, X. TW-FCM: An Improved Fuzzy-C-Means Algorithm for SPIT Detection. In Proceedings of the 2018 27th International Conference on Computer Communication and Networks (ICCCN), Hangzhou, China, 30 July–2 August 2018; pp. 1–9. [CrossRef]
6. Gad, A.F. Comparison of signaling and media approaches to detect VoIP SPIT attack. In Proceedings of the 2018 International Conference on Innovative Trends in Computer Engineering (ITCE), Aswan, Egypt, 19–21 February 2018; pp. 56–62. [CrossRef]
7. Xie, T.; Li, C.; Tang, J.; Tu, G. How Voice Service Threatens Cellular-Connected IoT Devices in the Operational 4G LTE Networks. In Proceedings of the 2018 IEEE International Conference on Communications (ICC), Kansas City, MO, USA, 20–24 May 2018; pp. 1–6. [CrossRef]
8. Muttavarapu, A.S.; Dantu, R.; Thompson, M. Distributed Ledger for Spammers' Resume. In Proceedings of the 2019 IEEE Conference on Communications and Network Security (CNS), Washington, DC, USA, 10–12 June 2019; pp. 1–9. [CrossRef]
9. Koilada, D.V.S.R.K. Strategic Spam Call Control and Fraud Management: Transforming Global Communications. *IEEE Eng. Manag. Rev.* **2019**, *47*, 65–71. [CrossRef]
10. Toyoda, K.; Park, M.; Okazaki, N.; Ohtsuki, T. Novel Unsupervised SPITters Detection Scheme by Automatically Solving Unbalanced Situation. *IEEE Access* **2017**, *5*, 6746–6756. [CrossRef]
11. Sengar, H.; Wang, X.; Nichols, A. Call Behavioral Analysis to Thwart SPIT Attacks on VoIP Networks. In *Security and Privacy in Communication Networks: Proceedings of the 7th International ICST Conference, SecureComm 2011, London, UK, 7–9 September 2011*; Revised Selected Papers; Rajarajan, M., Piper, F., Wang, H., Kesidis, G., Eds.; Springer: Berlin/Heidelberg, Germany, 2012; pp. 501–510. [CrossRef]
12. Azad, M.; Morla, R.; Arshad, J.; Salah, K. Clustering VoIP caller for SPIT identification. *Secur. Commun. Netw.* **2016**, *9*, 4827–4838. [CrossRef]
13. Morla, M.A.A.R. Early identification of spammers through identity linking, social network and call features. *J. Comput. Sci.* **2017**, *23*, 157–172.
14. Shin, D.; Ahn, J.; Shim, C. Progressive multi gray-leveling: A voice spam protection algorithm. *IEEE Netw.* **2006**, *20*, 18–24. [CrossRef]
15. Bokharaei, H.K.; Sahraei, A.; Ganjali, Y.; Keralapura, R.; Nucci, A. You can SPIT, but you can't hide: Spammer identification in telephony networks. In Proceedings of the 2011 Proceedings IEEE INFOCOM, Shanghai, China, 10–15 April 2011; pp. 41–45. [CrossRef]
16. Iranmanesh, S.A.; Sengar, H.; Wang, H. A Voice Spam Filter to Clean Subscribers' Mailbox. In *Security and Privacy in Communication Networks*; Keromytis, A.D., Di Pietro, R., Eds.; Springer: Berlin/Heidelberg, Germany, 2013; pp. 349–367.
17. Strobl, J.; Mainka, B.; Grutzek, G.; Knospe, H. An efficient search method for the content-based identification of telephone-SPAM. In Proceedings of the 2012 IEEE International Conference on Communications (ICC), Ottawa, ON, Canada, 10–15 June 2012; pp. 2623–2627.

18. Shah, M.; Harras, K. Hitting Three Birds with One System: A Voice-Based CAPTCHA for the Modern User. In Proceedings of the 2018 IEEE International Conference on Web Services (ICWS), San Francisco, CA, USA, 2–7 July 2018; pp. 257–264. [CrossRef]
19. Quittek, J.; Niccolini, S.; Tartarelli, S.; Stiemerling, M.; Brunner, M.; Ewald, T. Detecting SPIT Calls by Checking Human Communication Patterns. In Proceedings of the 2007 IEEE International Conference on Communications, Glasgow, Scotland, 24–28 June 2007; pp. 1979–1984. [CrossRef]
20. Soupionis, Y.; Koutsiamanis, R.A.; Efraimidis, P.; Gritzalis, D. A Game-Theoretic Analysis of Preventing Spam over Internet Telephony via Audio CAPTCHA-Based Authentication. *J. Comput. Secur.* **2014**, *22*, 383–413. [CrossRef]
21. Reaves, B.; Blue, L.; Abdullah, H.; Vargas, L.; Traynor, P.; Shrimpton, T. AuthentiCall: Efficient Identity and Content Authentication for Phone Calls. In Proceedings of the 26th USENIX Security Symposium (USENIX Security 17), Vancouver, BC, Canada, 16 August 2017; USENIX Association: Vancouver, BC, Canada, 2017; pp. 575–592.
22. Su, M.; Tsai, C. Using data mining approaches to identify voice over IP spam. *Int. J. Commun. Syst.* **2015**, *28*, 187–200. [CrossRef]
23. Hansen, M.; Hansen, M.; Moller, J.; Rohwer, T.; Tolkmit, C.; Waack, H. Developing a legally compliant reachability management system as a countermeasure against spit. In Proceedings of the Third Annual VoIP Security Workshop, Berlin, Germany, 1–2 June 2006.
24. Balasubramaniyan, V.A.; Ahamad, M.; Park, H. CallRank: Combating SPIT using call duration, social networks and global reputation. In Proceedings of the Fourth Conference on Eamil and Anti-Spam (CEAS 2007), Mountain View, CA, USA, 2–3 August 2007.
25. Azad, M.; Morla, R. Caller-REP: Detecting Unwanted Calls with Caller Social Strength. *Comput. Secur.* **2013**, *39*, 219–236. [CrossRef]
26. Kolan, P.; Dantu, R. Socio-technical Defense Against Voice Spamming. *Acm Trans. Auton. Adapt. Syst.* **2007**, *2*. [CrossRef]
27. Wang, F.; Wang, F.R.; Huang, B.; Yang, L.T. ADVS: A reputation-based model on filtering SPIT over P2P-VoIP networks. *J. Supercomput.* **2013**, *64*, 744–761. [CrossRef]
28. Kim, H.J.; Kim, M.J.; Kim, Y.; Jeong, H.C. DEVS-Based modeling of VoIP spam callers' behavior for SPIT level calculation. *Simul. Model. Pract. Theory* **2009**, *17*, 569–584. [CrossRef]
29. Wu, Y.; Bagchi, S.; Singh, N.; Wita, R. Spam detection in voice-over-IP calls through semi-supervised clustering. In Proceedings of the 2009 IEEE/IFIP International Conference on Dependable Systems Networks, Lisbon, Portugal, 29 June–2 July 2009; pp. 307–316.
30. Chikha, R.; Abbes, T.; Chikha, W. Behavior-based approach to detect spam over IP telephony attacks. *Int. J. Inf. Secur.* **2016**, *15*, 131–143. [CrossRef]
31. Ofcom. *Statistical Release Calender*; Technical Report; Ofcom: London, UK, 2019.
32. Javed, I.T.; Toumi, K.; Crespi, N. TrustCall: A Trust Computation Model for Web Conversational Services. *IEEE Access* **2017**, *5*, 24376–24388. [CrossRef]
33. Nanavati, A.; Gurumurthy, S.; Das, G.; Chakraborty, D.; Dasgupta, K.; Mukherjea, S.; Joshi, A. On the Structural Properties of Massive Telecom Call Graphs: Findings and Implications. In Proceedings of the 15th ACM International Conference on Information and Knowledge Management, Arlington, VA, USA, 6–11 November 2006; pp. 435–444.
34. Melo, P.; Akoglu, L.; Faloutsos, C.; Loureiro, A. Surprising Patterns for the Call Duration Distribution of Mobile Phone Users. In *Machine Learning and Knowledge Discovery in Databases, Proceedings of the European Conference, ECML PKDD 2010, Barcelona, Spain, 20–24 September 2010*; Part III; Springer: Berlin/Heidelberg, Germany, 2010; pp. 354–369.
35. Guo, J.; Liu, F.; Zhu, Z. Estimate the Call Duration Distribution Parameters in GSM System Based on K-L Divergence Method. In Proceedings of the 2007 International Conference on Wireless Communications, Networking and Mobile Computing, Shanghai, China, 21–25 September 2007; pp. 2988–2991. [CrossRef]