VoIP Spam Detection using Machine Learning

Himanshu Raghuwanshi, Ravula Praveen, Taruni Renuka and Hariharan

Mentor: Dr. Mayank Swarnkar

ABSTRACT

Spam Over Internet Telephone can become a serious threat within the close to the future due to the growing number of VOIP users.We tend to propose a model that uses the time duration (length) of calls between two users to differentiate normal callers and spam callers.Here, we define a process to notice spammers in VoIP by classifying differences in the Call Graph. This directed, by using call data records weighted graph and it is created where the set of separating call parameters are used to derive weights on the edges.In this Voice over Internet Protocol (VOIP) spam Detection, we've bestowed associate approach merging protocols and characteristics of callers. This system provides us a straight forward and a simple way to use call period as associate automatically selected model based on human behaviour.

1. INTODUCTION

Voice Over internet Protocol (VoIP) is a group of number of co-existing and challenging protocols for delivering of voice communications over IP networks such as internet. [1] VoIP has greatly changed the way telephony data is communicated by using IP networks to route packets containing small portions of voice communications. Session Initiation Protocol (SIP) is used to start, uphold and tear-down calls when completed. Real-time Transport Protocol (RTP) is used for transmitting audio in the form of packets over the IP network. This technology is attracting criminals as it is problematic to confirm the user's own identification. VoIP is additionally obtainable on several Internet access devices and personal (Private) computers, Calls and text messages that will be sent over Wi-Fi.[19] VoIP permits modern communications technologies which includes telephones, smartphones, video and voice conferencing, email and detections that are to be to be combined using a single unified communication system.However, these ways use uniquely average values of options and therefore they fail to figure if a determined spam user maintains these averages by artificial calls.Based on call duration to differentiate between genuine users and spammers.[17]These spam calls not only convey economic damage to the users of the telephony but also irritate them with unsolicited ringing alerts. Therefore, It is mandatory for the operators to block the internet telephony spammers at the control of the network so that it will increase trust of their clients (customers). We observed that a spammer will naturally receive no calls or few calls from other different users.[2] The problem of spam is increasing day-by-day and up to date results indicate that of all the e-mail that's current within the net straight away, as high as eightieth of that's spam (junk or unsought messages). Network engineers can capture and analyse VoIP call packets using wireshark in order to identify suspicious calls. Wireshark also has VoIP extension to replay audio captured in RTP packets.

Wireshark also has feature to detect VoIP calls from the trace. From Menu go to 'Telephony' and select 'VoIP calls'. A new window appears which lists all the calls in the trace along with its related information. Audio from the RTP streams can be played for specific VoIP call using "Play streams button". Flow of a specific VoIP call can be viewed in a graphical manner using the 'Flow Sequence' button.

This interaction between users is represented as a weighted graph and to identify the spam users we identify differences in the graph structure[22]. The idea of using anomalies is motivated by the fact that spam users usually have different interaction patterns like higher calling frequency, large number of short duration calls, etc., which are used to descend appropriate weights on edges help differentiate these users of spam and normal.

The Benefits of a VoIP communication System are - Advanced options and flexibility. -Affordable and add-ons you'll get. -More secure than your telephone landline. VoIP will share ideas, information and thoughts in period of time. You can additionally accelerate projects with instant collaboration tools like Instant electronic communication (Messaging), group chats, and video sharing.

The constant evolution of the VoIP technology beside the up to date contemporary changes within in the VoIP market sets the VoIP trends.[14] This ascension is because of easy availability of internet services. As here internet is the main demand of the VoIP market, individuals with easy accessibility to internet are currently selecting VoIP over the traditional telephone system.

Some of VoIP Technology Trends in 2019, United Communication as a service can increase Adoption. 5G will enter the mainstream. Increased use of mobile unified communication. Artificial intelligence is going to transform customer experiences Increased trouble about security. Smarter VoIP assistants.

To make VoIP over wireless associate economically possible solution and a variety of technical challenges should be self-addressed. One among the most essential is the bandwidth efficiency.[12] For mobile wireless communications information measure remains a scarce resource and it's of vital importance that is to be used efficiently. If today's circuit-switched cellular system will support over a range of VoIP users otherwise the spectrum prices would be prohibited.

In the coming years telecom providers must start thinking about VoIP Spam and keep this problem in mind while designing new telephony systems.Here we propose a model just by a data set and going to detect spam calls and normal.

2. RELATED WORKS

These are some techniques which are related to VoIP Spam:

White Listing: [3] A white listing is a list of user ID's which are marked to be 'good-guys'. Normally the initiator who's user ID is on the white list of the recipient gets a special treatment. In most implementations this gets down to bypassing further anti-Spam mechanisms. A white list can either be a private list (i.e. buddy list) or a group list. Group lists are used by multiple users and therefore are stored centrally and are accessible for all authorized users. Private lists, which are personal (every user has a list), are likely to be smaller and could be stored either in the network or on user equipment.

Black Listing: [3] A black listing is a list of user ID's which are marked to be 'bad-guys'. Normally the initiator who's user ID is on the black list of the recipient gets a special treatment. In most implementations this gets down to either blocking or applying a stronger anti-Spam mechanism. Private lists, which are personal (every user has a list), are likely to be smaller than group lists and could be stored either in the network or on user equipment. Although a black list can be either a private list or a group list, the most implementations are group lists.

Human involvement was required to identify unwanted callers. Even though this technique can detach spammers, it suffers from a major drawback.[5] Trust and reputation in this system were assigned to an entire domain rather than individual users. So, a particular domain has a lot of spammers and a few authentic users, those legitimate users would be castigated along with the rest of the spammers. A callee can decide to answer or reject the call based on this mechanism. However, Call Rank produces false positives when a new legitimate user joins the VoIP system.[5] Because he has no social network linkage in that system therefore all his calls will be classified as spam calls. Due to its centralized there are some problems. First, the users are usually reluctant to give negative rating because of other's negative rating. Second, if a user has a bad reputation rating, it will remove its old identity and the third problem is that user can increase their reputation artificially by creating fake identities and these fake identities will give themselves high rating. Each user is responsible for evaluating a faith of other user based on their direct interactions.

3. PROPOSED METHOD

In this section we describe our proposed method VoIP spam detection using machine learning. Machine learning model use social interaction among users to detect spam over internet telephony (SPIT).
[4] we have to separate SIP (Session Initiation Protocol) responses in the data set which are in pcap format. SIP responses are the answer to SIP requests, which means, that the response contains the information and call duration etc. we have Some basic information on SIP session in Section 3.1 so that we can understand why we separated SIP responses.

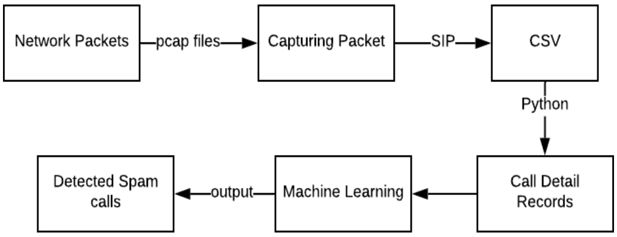
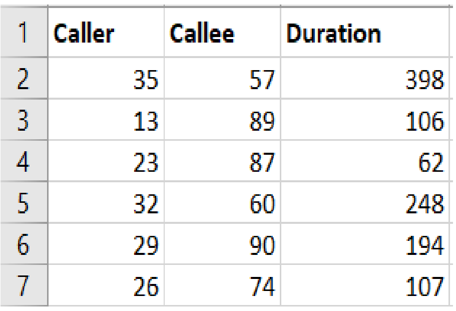


Fig. 1: Flow Chart

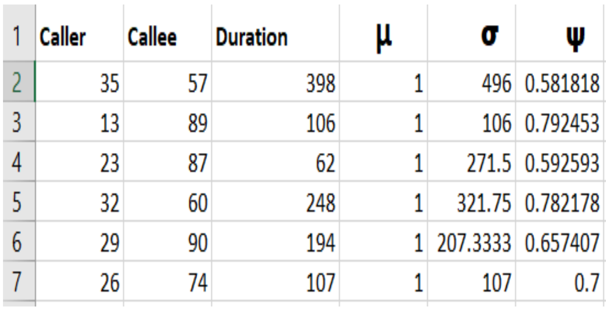
It has generally three stages: First extracting SIP responses from pcap files and by using wireshark over linux operating system and converting them into csv format.



1	Caller	Callee	Duration
2	35	57	398
3	13	89	106
4	23	87	62
5	32	60	248
6	29	90	194
7	26	74	107

Fig. 2: CSV file

Secondly by using python script on csv file we have developed our classification parameters Call Detail Records (CDR).



1	Caller	Callee	Duration	μ	σ	ψ
2	35	57	398	1	496	0.581818
3	13	89	106	1	106	0.792453
4	23	87	62	1	271.5	0.592593
5	32	60	248	1	321.75	0.782178
6	29	90	194	1	207.3333	0.657407
7	26	74	107	1	107	0.7

Fig. 3: Call Detail Records

After that we have used our classification model "Random forest" for detecting spam over VoIP calls.

3.1. Session Initiation Protocol

In this section we describe our proposed model and now by using wireshark [4] we have to separate SIP (Session Initiation Protocol) responses in the data set which are in pcap format. SIP responses are the answer to SIP requests, which means, that the response contains the information and call duration etc. [4] As you can see in Fig. 4 User Agent 'A' initiates the session establishment, by sending an 'Invite' request to User Agent 'B'. The 'Invite' request is the first component of the three way handshake. User Agent 'B' reacts and sends the provisional response 'Trying' back to User Agent 'A', followed by the provisional response 'Ringing', which indicates, that the phone of user B rings. As 'Trying' and 'Ringing'

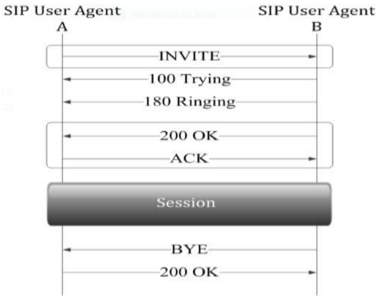


Fig. 4: SIP Session

are both provisional (optional) responses, they are not considered to be part of the three way handshake[4]. As soon as user B picks up the phone, response OK is generated by User Agent 'B' and sent to User Agent 'A'.User Agent 'A' answers with the sending of an ACK, which indicates that he is still willing to communicate. As the messages 'OK' and ACK are second and third element of the three way handshake, and all session parameters are exchanged, the session is established. In our example User Agent B terminates the session with a 'BYE' request, which is answered by User Agent 'A' with a OK response.

3.2. Call Parameters

In this section, we evaluate the presentation of the approach which we were proposed for the evaluation. In Addition to present this, we also discussed the call parameters and weighted graphs in order to know the performance of detection of Spammers and Normal calls. Here we considered three types of parameters

3.2.1. Successful call rate

By successful calls we get the ratio of calls (successful calls) made by a caller i to the number of calls attempted by the caller to that another use j. We denote successful call rate as mu and its value is calculated as in the below equation. The value mu lies between 0 and 1. if mu is 0 then it indicates that there is no successful calls are made by the user and when it shows 1 then it indicates that the calls are successful.

$$\mu_{ij} = \frac{Successfull\ calls\ by\ user\ i\ to\ user\ j}{Total\ calls\ initiated\ by\ user\ i\ towards\ user\ j} \quad (1)$$

3.2.2. Average talk time per call

In this parameter we measure the average duration time duration of each call from user I to j. we use sigma to denote average talk time per calls and its vale us calculated by the below equation and the value of sigma is greater than or equal to 0.

$$\sigma_{ij} = \frac{Total\ Talk - time\ in\ calls\ from\ user\ i\ to\ user\ j}{Total\ successful\ calls\ made\ by\ user\ i\ to\ user\ j} \quad (2)$$

3.2.3. User role in Calls

It is the ratio of number of times user u caller and the number of times user u called. It is calculated by the below equation.

$$\psi_u = \frac{Number\ of\ times\ user\ u\ is\ a\ caller}{Number\ of\ Times\ user\ \ u\ is\ a\ callee} \quad (3)$$

4. EXPERIMENT AND RESULT

4.0.1. Simulation Parameters and Datasets

Parameter	Value	Description
Normal Call Duration (sec).	More than 20 seconds	Normal Distribution
Spam Call Duration (sec).	Less than 15 seconds	Normal Distribution
Number of Normal calls.	445336	labelled as 1
Number of Spam calls	154664	labelled as 0

Table 1: Simulation Parameters

Sample Call Data Records:

Caller	Calle	Duration	μ	σ	ψ	Label
4252	147	77	1	357.5	2.6520	1
47	64	513	0.77	177	16.760	0
4096	84	286	1	324	2.1100	1
5512	1236	12	1	12	639.00	0
35	48	418	1	262	0.5800	0
1157	3190	129	0.87	125	0.7642	1
46	80	6	0.75	8.33	15.1923	0
1555	6691	10	1	10	9.9060	0

Table 2: Sample Call Data Records

4.1. Training Set:

PARAMETERS	VALUE
Total calls	600000
Normal calls	445336
Spam calls	154664
Total No. of VoIP callers	10000

Table 3: Parameters for Traning

From the above Table.3 These are the some parameters which are in Testing Set and here the total calls is 600000 where as normal calls 445336 and spam calls 154664, here the total no of VoIP users are 10000.

4.2. Testing Set

PARAMETERS	VALUE
Total calls	10000
Normal calls	4000
Total No. of VoIP callers	100

Table 4: Parameters for Testing

From the above Table.4 These are the some parameters which are in Testing Set and here the total calls is 10000 where as normal calls 100 and here the total no of VoIP users are 100.

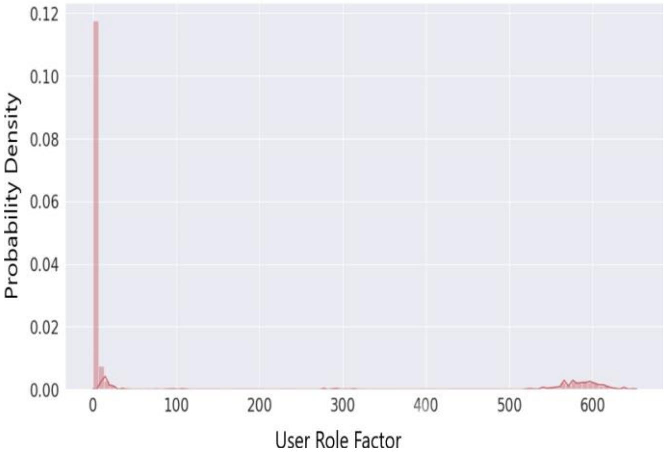


Fig. 5: User role in calls

A density plot shows the distribution of a numerical variable. By the above graphical representation it conveys that the user role in the call. It’s the graph plot that flows- PSI against its in terms of the density. On X-axis the normal users comes under the range of (0-less than 3.0),this indicates that the normal users are lies in the specified range as per the graphical representation and in case of the spammers the PSI against the density it lies above the 3.0 and it shoots upto 600 and above. The spam calls have a less density while compared to the normal calls,thats because of the user role of the spam caller.Usually the Normal calls will be visualed around the (0.5-2).

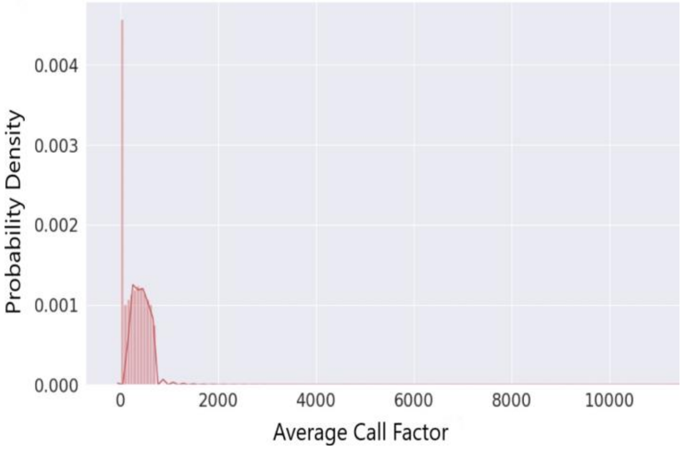


Fig. 6: Average talk time per call

This above graph indicates that the spammer role in the talktime parameter.Since the Spammer has a very much lower talktime than the Normal User. The density of the Normal User is Promoted to a higher range than the Spammer. This graph conveys that the total area which is bordered as Normal users gives the total area when calculates it gives a UNIT output Other than the bordered/ outlayered sorts are spammers.

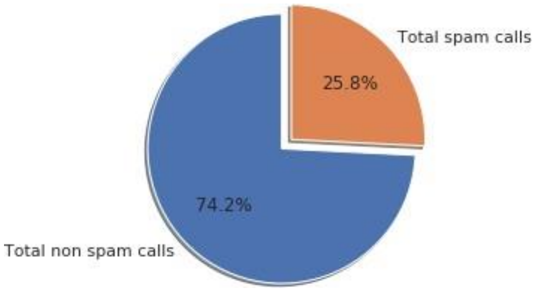


Fig. 7: No. of Calls

The above pie chart conveys that the total number of spam calls over the total number of normal calls.

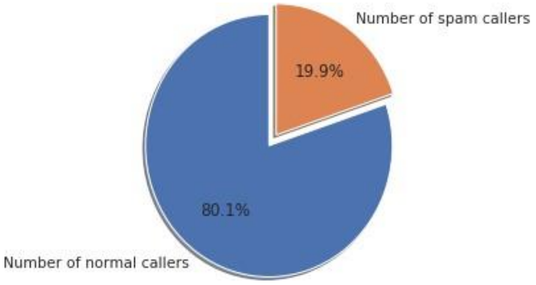


Fig. 8: No. of Callers

The above pie chart conveys that the total number of spam callers over the total number of normal callers.

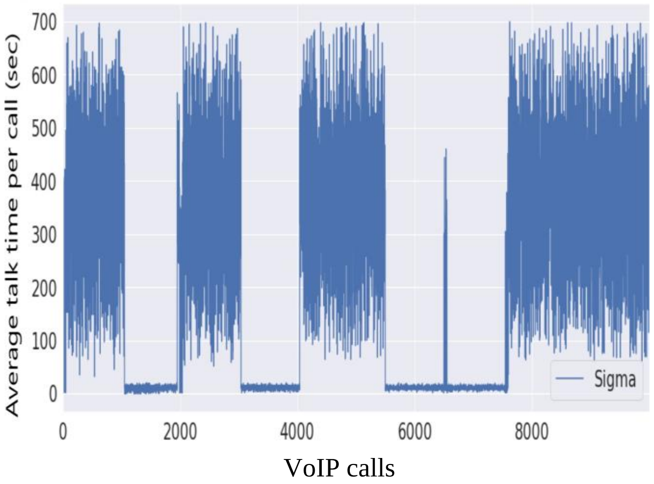


Fig. 9: sigma test

The above bar line plot pass the information that the SIGMA value for the call between the Normal users and the Spam users. It conveys that the SIGMA factor value is furthermore lower for the Spam calls (ie. 0-7.5),while the SIGMA value for the normal calls varies from (50-800)

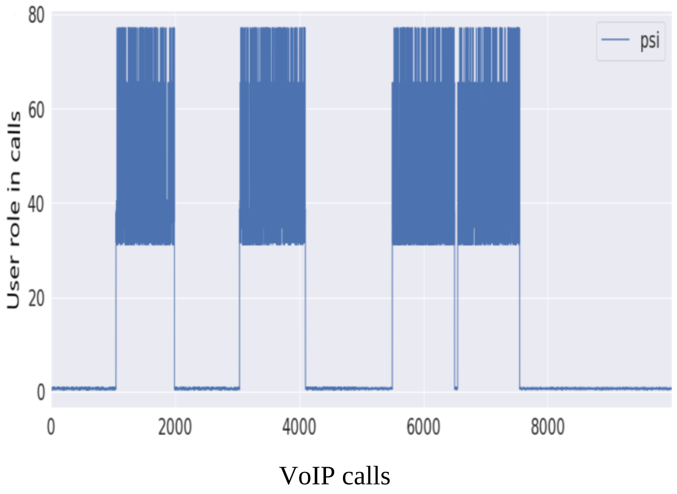


Fig. 10: Psi test

The above bar graph pass us the information that the PSI value for the calls between the Normal users and the Spam users. It conveys that the PSI factor value is too high for the Spam calls made by the spammers (ie.30-100),while the PSI value for the Normal calls are further small which are from (0-2).

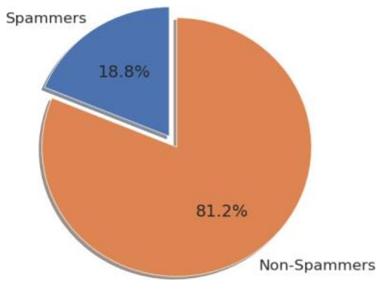


Fig. 11: Callers test

The above pie chart conveys that the total number of spam callers over the total number of normal callers

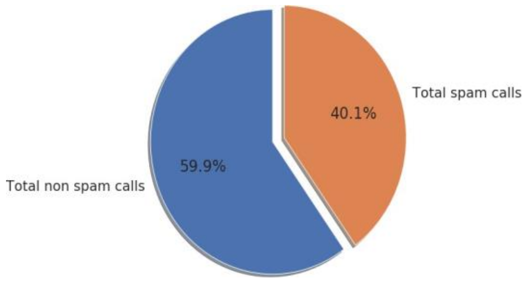


Fig. 12: Calls test

The above pie chart conveys that the total number of spam calls over the total number of normal calls

5. Analysis:

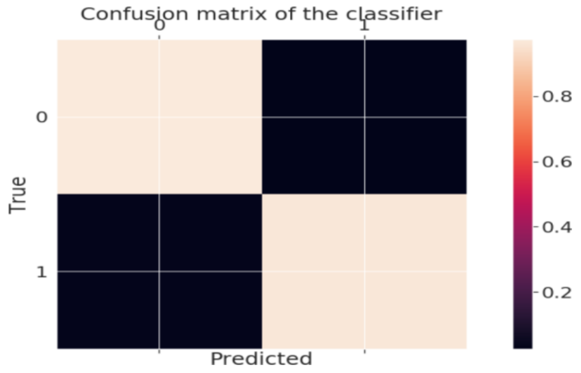
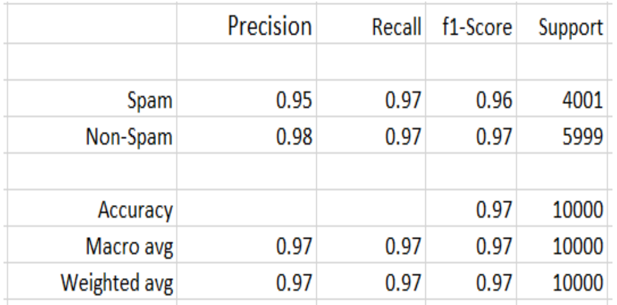


Fig. 13: Analysis



	Precision	Recall	f1-Score	Support
Spam	0.95	0.97	0.96	4001
Non-Spam	0.98	0.97	0.97	5999
Accuracy			0.97	10000
Macro avg	0.97	0.97	0.97	10000
Weighted avg	0.97	0.97	0.97	10000

Fig. 14: Confusion Matrix

This Analysis classification report is used to know the quality of estimations from a classification algorithm. By this we can know how many predictions are True and how many predictions are False. Fig.14 is the metrices classification report.

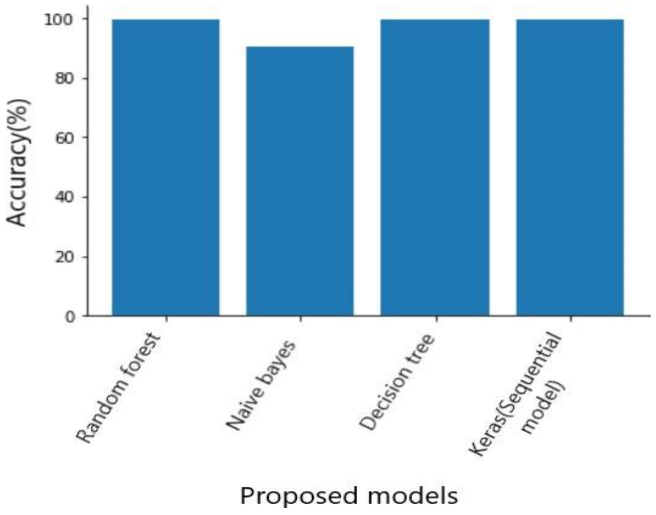


Fig. 15: Accuracy for different models

Many techniques have been developed to help experts better understand classification models.A classification model tries to draw some conclusion from the input values given for training. It will predict the class labels/categories for the new data. We have analysed our training and testing dataset over different classification models such as Naive Bayes, Decision tree. We have also built a deep learning model with Keras API using a sequential model for classification of our training and testing dataset. Results of accuracy for different models and time for execution of each model is depicted in graphs Fig.15 and Fig.16:

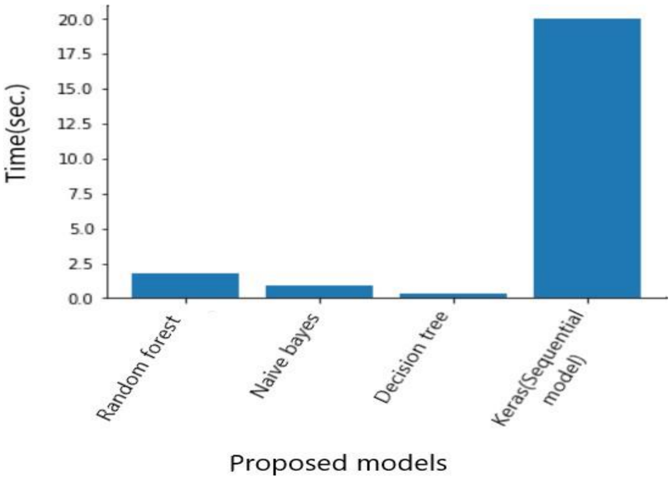


Fig. 16: Time graph

6. Discussion

Since telephony systems are moving to 'all-IP' and IP networks suffer from a trust problem, a lot of threats which apply to an IP network suddenly also apply to telephony.[3] As the use of IP based telephony is growing it is more and more attractive for a new type of Spamming, VoIP Spamming. Since in a VoIP network the costs (i.e. time and money) for the initiator are lower than the costs (i.e. time and money) for the recipient, VoIP Spam is a potential problem.

The present nature of Voice over Internet Protocol network requires that the SPIT (Spam over Internet Telephony) callers should be exhortation from calling during the call set-up stage instead of blocking during the exchange of speech contents after the call set-up[16]. The recognition of Spam over intrnet telephony through the call arrangement improves customer satisfaction of not getting useless call ringing and improves resource utilisation kept for the genuine callers. [8] The content-based SPIT detection is not possible choice as it needs system resources for speech recognition and speech processing, an updated speech dataset of spammers and Normal calls (Non-Spammers) for real-time data processing and is additionally be difficult to be applied to the encrypted speech.[10] Moreover, processing speech is against the user data protection. The list-based methods need much maintenance when calls are received from various sources.[9] The reputation-based approaches computes status of the caller by getting feedback from the callee or uses average call duration, but they trust on callee's for making final result about rejecting or accepting the call.

7. Conclusion

Computer networks are facing many threats such as VoIP spam etc without the awareness of the users.[9] Network forensics is required as many of the methods implemented for network security are not effective enough to detect all of the attacks on the network. Wireshark is the one of the most effective-tool for capturing and analysing packets in network forensics because of its rich features and its ability to display information as detailed as possible. In this Voice over Internet Protocol (VOIP) spam Detection, we've associated an approach that merges protocols and characteristics of callers. This system provides us a straight forward and a simple way to use call period (Duration) as associate automatically selected based on the caller and Callee.[13] The projected technique is additionally enforced in the line with decision behaviour and human reasoning. However, the genuine user may be redoubled with calls lasting long enough. This supports the bidirectional communication characteristic of a genuine user decision. To an extent the Detection we tend to additional projected a trust propagation methodology just in case a caller and callee don't have a direct relationship. Supported accurate simulation results,[7] we found that the predictable procedure will sight all Spam Over Internet Telephony (SPIT) completely when some learning period keeping a short false positive rate. We also verified that when the number of spammers was increased then the accuracy of spam and genuine call detection were still higher than 95 and 98 percentage respectively. This relationship features among the nodes in the network will not affect the detection accuracy. Here we conclude that our proposed method can be applied to real Voice over Internet Protocol Network.

References

[1] Goode, B. (2002). Voice over internet protocol (VoIP). Proceedings of the IEEE, 90(9),1495-1517

[2] Dantu, Ram, and Prakash Kolan. "Detecting Spam in VoIP Networks." SRUTI 5 (2005): 5-5.

[3] Mathieu, Bertrand, Saverio Niccolini, and Dorgham Sisalem. "SDRS: a voice-over-IP spam detection and reaction system." IEEE Security Privacy 6, no. 6 (2008): 52-59.

[4] Rosenberg, Jonathan, Henning Schulzrinne, Gonzalo Camarillo, Alan Johnston, Jon Peterson, Robert Sparks, Mark Handley, and Eve Schooler. "SIP: session initiation protocol." (2002).

[5]Chaisamran, Noppawat, Takeshi Okuda, and Suguru Yamaguchi. "Trust-based voip spam detection based on calling behaviors and human relationships." Journal of Information Processing 21, no. 2 (2013): 188-197.

[6]Reumann, J., Saha, D., Shae, Z.Y. and Sripanidkulchai, K., Abbott Laboratories and International Business Machines Corp, 2007. System and method for spam detection. U.S. Patent Application 11/334,920.

[7]Piche, C., Eyeball Networks Inc, 2010. Method and system to prevent spam over internet telephony. U.S. Patent Application 12/067,168.

[8]Quittek, Juergen, Saverio Niccolini, Sandra Tartarelli, and Roman Schlegel. "On spam over internet telephony (SPIT) prevention." IEEE Communications Magazine 46, no. 8 (2008): 80-86.

[9]Rao A, McRae M, Harrington K, Huotari A, inventors; Cisco Technology Inc, assignee. Method and system for deterring SPam over Internet Protocol telephony and SPam Instant Messaging. United States patent application US 11/203,449. 2007 Feb 22.

References

[10]MacIntosh, Robert, and Dmitri Vinokurov. "Detection and mitigation of spam in IP telephony networks using signaling protocol analysis." In IEEE/Sarnoff Symposium on Advances in Wired and Wireless Communication, 2005., pp. 49-52. IEEE, 2005.

[11]Rebahi, Yacine, Dorgham Sisalem, and Thomas Magedanz. "Sip spam detection." In International Conference on Digital Telecommunications (ICDT'06), pp. 68-68. IEEE, 2006.

[12]Huang, H., Yu, H.T. and Feng, X.L., 2009, November. A spit detection method using voice activity analysis. In 2009 International Conference on Multimedia Information Networking and Security (Vol. 2, pp. 370-373). IEEE.

[13]Kim, Hyung-Jong, Myuhng Joo Kim, Yoonjeong Kim, and Hyun Cheol Jeong. "DEVS-Based modeling of VoIP spam callers' behavior for SPIT level calculation." Simulation Modelling Practice and Theory 17, no. 4 (2009): 569-584.

[14]Vinokurov, Dmitri, and Robert W. MacIntosh. "Detection and mitigation of unwanted bulk calls (spam) in VoIP networks." U.S. Patent 7,307,997, issued December 11, 2007.

[15]Jones, Wesley Stuart, Timothy Cotton, and Robert Victor Holland. "Voice over internet protocol telephone system and method." U.S. Patent 6,141,341, issued October 31, 2000.

[16]Rao, Anup, Matthew McRae, Kendra Harrington, and Allen Huotari. "Method and system for deterring SPam over Internet Protocol telephony and SPam Instant Messaging." U.S. Patent Application 11/203,449, filed February 22, 2007.

[17]Piche, Christopher. "Method and system to prevent spam over internet telephony." U.S. Patent Application 12/067,168, filed September 9, 2010.

[18]Shaw, Urjashee, and Bobby Sharma. "A survey paper on voice over internet protocol (VOIP)." International Journal of Computer Applications 139, no. 2 (2016): 16-22.

[19]Dritsas, Stelios, John Mallios, Marianthi Theoharidou, Giannis F. Marias, and Dimitris Gritzalis. "Threat analysis of the session initiation protocol regarding spam." In 2007 IEEE International Performance, Computing, and Communications Conference, pp. 426-433. IEEE, 2007.

[20]Baumann, Rainer, Stéphane Cavin, and Stefan Schmid. "Voice over IP-security and SPIT." Swiss Army, FU Br 41 (2006): 1-34.

[21]Hwang, Lin Yuh-Ing, Leroy Lacy, and Li Ling. "Method to detect spam over internet telephony (SPIT)." U.S. Patent 8,141,152, issued March 20, 2012.

[22]Bai, Y., Su, X. and Bhargava, B., 2009, June. Detection and filtering Spam over Internet Telephony—a user-behavior-aware intermediate-network-based approach. In 2009 IEEE International Conference on Multimedia and Expo (pp. 726-729). IEEE.