Enhance Approach for Handling Spam Calls in VOIP Scenario

[1]Khushbu Patel, [2]Kalpesh Patel, [3] KrunalSuthar
[1]M. Tech Student, [2,3]Assistant Professor,
[1]Department of Computer Engineering, LCIT, Bhandu. India.
[2] Department of Computer Engineering, LCIT, Bhandu. India
[3]Department of Computer Engineering, SPCE, Visnagar. India.

Abstract—Voice over Internet protocol(VOIP) has become a very popular. It is a methodology and group of technology for the delivery of a voice communication and multimedia session over Internet protocol network such as Internet. VOIP is the main protocol which help to make a call. It is used SIP (Session Initiation Protocol) protocol and PSTN (Public Switched Telephony Network) and other protocol. It is allows telephone calls to be made over digital computer network including the Internet. VOIP's main advantage is audio and video call communication.

But some problems are create in VOIP system like spam calls. Attackers are hack the numbers and get all details, security etc. In this paper, various methods for security and unsolicited calls referred as pam over VOIP to detection and prevention of unsolicited calls using call parameters.

Keywords—VOIP, White list, Black list, CAPTCHA method, Feedback.

I. INTRODUCTION

Voice over Internet protocol (VOIP) is a technology which uses packet switched network to transmit real voices via the Internet. This technology also can referred as IP telephony. VOIP is a family of technology that can offer both voice communication and multimedia sessions over internet protocol (IP) network. This technology is rapidly adopted by consumers and enterprises since it offers more functionalities and higher flexibility than traditional telephony. With increase he VOIP application, VOIP threats appear and become more and more a problem spam calls, attackers are hack numbers and get all details, Security etc. SPIT, known an unsolicited and unwanted calls send via VOIP networks.

White list and Black list:

White list

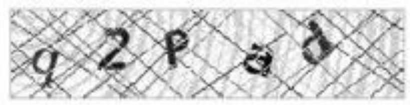
White list are opposite of the black list. There are list which contain the addresses of valid users. The communication requests from these addresses are not blocked. White list are also vulnerable to spoofing but that can be prevented with strong authentication mechanism. White list are useful in IM system due to the fact that they exist naturally in the form of buddy lists or contact list.

Black list

There are lists that contain address of known spammers and are usually maintained by spam filters. The address, comprise both username and the domains. In case of email, black list are not very effective because address can easily be forged and the spammer may come up with a spoofed address which can render the black lists useless. Even if the spammer does not forged address, he or she can get a new ‘from’ address, as email address are in abundant supply.

CAPTCHA Method

CAPTCHA (Completely Automated Public Turing Test to Tell Computers and Human Apart) uses the Turing test approach to determine whether the user and caller is human or machine. Email is one application that uses the CAPTCHA method to prevent spam entering the user’s mail box. The strength of this method and its success in preventing spam in email made it appealing as a means of preventing spam in VOIP applications. Figure 1 shows an example of CAPTCHA image.



[Fig 1. Example of CAPTCHA image]

II. RELATED WORKS

Security and perfomance is very challenging task in VOIP system because it provide distributed envioroment to the user for store personal data and details in mobile.But all information of use are not secure in some methods and algorithm. And privious authers are not give the perfect methods for detection and prevention for unsolicited calls.We have studied several such paper for reduce above problem.They are described as bellow:

Author at[1] proposed a model for unsupervised SPITers detection schema by adding artificial SPITers data to solve the unbalanced situation. The key contribution is to propose a novel way to automatically decide how much artificial data should be added. We show that classification performance is improved by means of computer simulation with real and artificial call log data sets.

In this paper [2] propose the system to detect SPIT attacks through behavior based approach. Our Framework operates in three steps:(1) collecting significant calls attributes by exploring and analyzing network traces using OPNET environment. (2) applying sliding windows strategy to properly maintain the caller profiles, and (3) classifying caller. This result of our expriments demostrat e the great performance of these methods.

This Paper Author [3] propose Anti-SPIT mechanism which is based on calculation of reputation using analysis of behaviors compared between normal users and SPITTERs for allow or block calls. Both the service provider and the Callee have role in the detection process. Also call list will be updated in time.

This Paper Author [4] discuss the problem of spam over IP telephony and investigate techniques which use the session Initiation Protocol (SIP) to reject likely nuisance callers. Existing techniques include content filtering, black lists, white lists, gray lists, call rate monitoring, IP/domain correlation, consent-based communications, reputation systems, address obfuscation, limited-use addresses, computational puzzles, payments at risk, legislation, circles of trust, centralized SIP providers, and authenticated identity. A new technique using a text-based Turning test is proposed and demonstrated to be compatible with the SIP protocol.

In this paper we propose an approach that assigns weight to features and determines which feature is more important than the others in classification of suspicious incoming calls. Once we select the best features, we can detect SPIT efficiently in less time. In this paper a SPIT detection algorithm based on user’s call behavior. Simulation results show the efficiency of four detection method and outline the most significant parameters. We find that the inspection of call duration allows to quickly and precisely SPIT messages.

III. COMPARISON OF VARIOUS RESEARCH SCHEMES

The table below shows a short comparison about the various schemes proposed by a researcher by taking different parameters. The table gives the description about the basic technique usedwith the benefits that researcher gets the limitations found in schemes.

Criteria Group →	Approach for handling spam calls in VOIP scenario.					Others
Individual Criteria → Providers ↓	White list and black list	CAPTCHA method	User’s Feedback	Call behavior	Call Duration	Call Classification
[1]	No	No	No	No	No	Yes
[2]	No	No	No	Yes	No	No
[3]	No	No	No	No	Yes	No
[4]	Yes	No	No	No	No	No
[5]	No	No	No	No	Yes	No
[6]	No	No	No	Yes	No	No

Table 1. Comparison study

IV. PROPOSED METHODOLOGY

Steps:-

Step 1: Start.

Step 2: Incoming Calls.

Step 3: Call checking in Black list.

Step 4: If it is found in black list so End call, else check in white list.

Step 5: If it is found in white list so send a call, else send the CAPTCHA.

Step 6: Compare the CAPTCHA reply.

Step 7: If the CAPTCHA answer is right so send a call, else reach to threshold value.

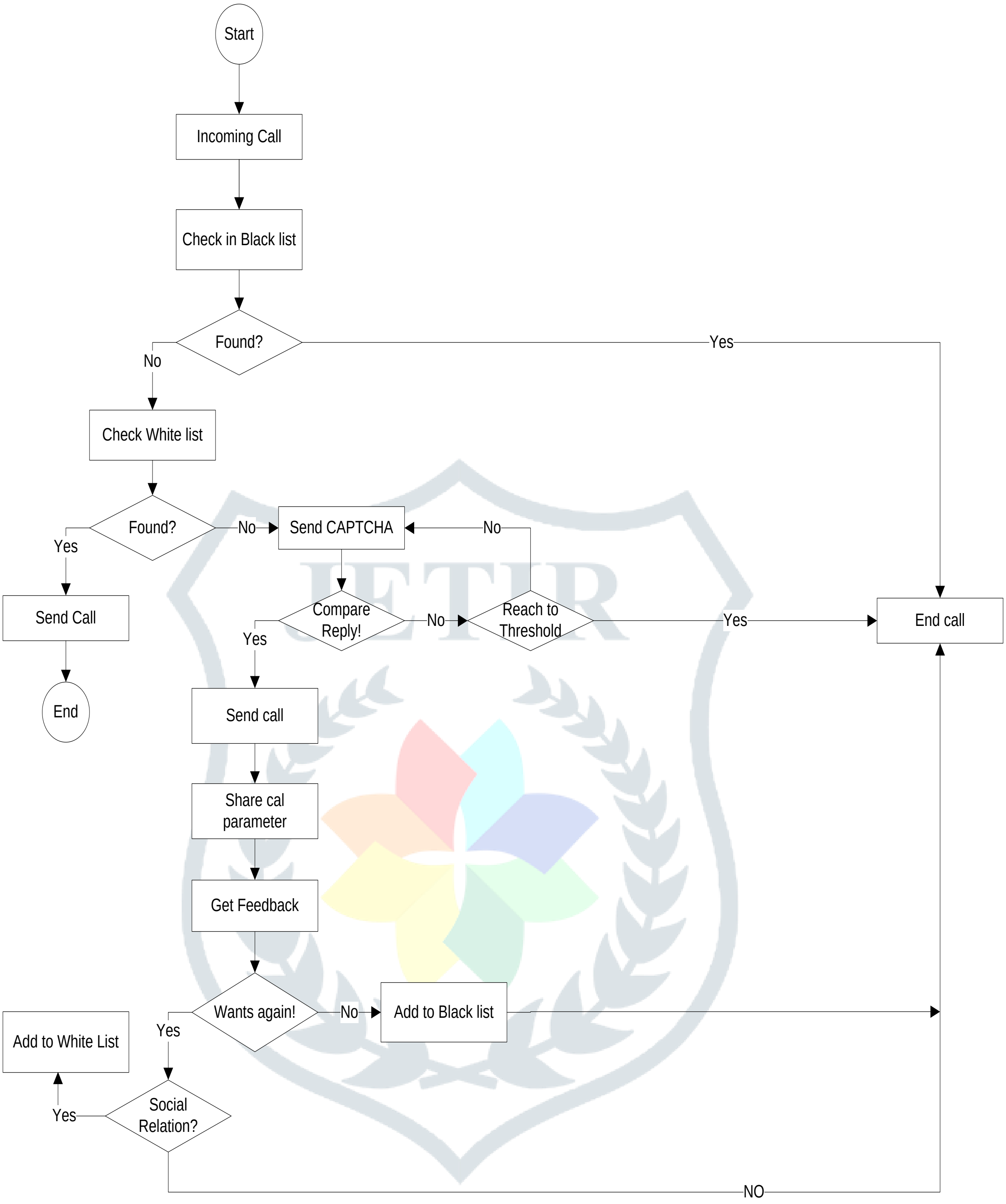
Step 8: If reach the threshold value so end the call, else go to step 5.

Step 9: After send a call then share call parameter and get feedback.

Step 10: If you wants to call again so check social relationship.

Step 11: If yes so put that number is in white list, else call end.

Step 12: Stop.



Main Aim is to solve problem related to unsolicited calls referred as spam over VoIP.Propose methodology work in various directions like detection and prevention of unsolicited call.We also use fundamental of users feedback which may decrease the time required to check history every time when session initiates.The proposed scheme not only stops the VoIP Spam calls but also increase the success rate while work on various dimension to stop unwanted calls.

Conclusion

In this paper we provides description about how to detect and prevent the unsolicited calls and unwanted calls. researcher used white list, black list, CAPTCHA method, user's feedback and its categories for solving various issues. In this paper track the calls details and stop the call accordingly and stop the automated generated calls. Use the multi dimentional mechanism to detect and prevent the spam calls. It is provide the high efficincy due to scalable system. White list and black list are used for cheching the valid and unvalid number. The CAPTCHA method can be applide in VOIP application.The researcher also argue that their method provides high security and call details protection to provider as well save the time for initiating call by decrese the spam calls.

REFERENCES

[1] Kentaroh Toyoda, Naonobu Okazaki, Tomoaki, “Novel unsuperwised SPITs detection scheme by automatically solving unbalanced situation” “In conference name, IEEE, 2017.

[2] RandaJabeur Ben Chikla, Tarek Abbes, Wassim Ben Chikla, Adel Bouhoula,” Behavior based approach to detect spam over IP telephony attacks”In reference name, SPRINGER, 2016.

[3] FaridehBarghi, Mohammad Hossein, YaghmaeeMoghadam “A comprehensive SPIT detection and prevention framework based on reputation model on call communication patterns” In conference name, IEEE,2014.

[4] Saeed Farooq Khan, Marius Portmann, Neil W. Bergmann,“VOIP spam prevention “In conference name, IEEE, 2013.

[5] Mina Amanian, Mohammad Hossein Yaghmaee, Hossein KhosraviRoshkhari,“New method for evaluating anti-spit in VoIP network” In conference name, IEEE, 2013.

[6] RandaJabeur Ben Chikha, Tarek Abbes, Adel Bouhoula,“A SPIT detection algorithm based on user’s call behavior” In conference name, IEEE, 2013.

[7] RandaJabeur Ben Chikla, Tarek Abbes, Adel Bouhoula,” Risk management for Spam over IP telephony using optimal countermeasure” “In conference name, IEEE, 2016.

[8] Joughan Lee, Kyumin Cho-chang Yong Lee-Seungioo Kim “ VOIP aware network attack detection based on statistics and behavior of SIP traffic” In reference name, SPRINGER, 2016.

[9] Ismail Ahmedy, Marius Portmann” Using CAPTCHAs to mitigate the Voip spam problem” In conference name, IEEE, 2010.

[10] Chen Hongchang, chenfucai, LiShaomei”A multilayered fusion method for SPITs detection” In conference name, IEEE, 2011.

[11] Hemant Sengar, Xinyuan Wang, Art Nichols” Thwarting spam over internet telephony(SPIT) attacks on VOIP network”In conference name, IEEE, 2011.

[12] Dirk Lentzen, Gary Grutzek, Heikoknospe, Christoph Porschmann”Content based detection and prevention of spam over IP telephony system design, prototype and first result”In conference name, IEEE, 2011.

13] NoppawatChaisamran,Takeshi Okuda, Gregory Blanc, SuguruYamaguchi”Trust based VOIP spam detection based call duration and human relationship”In conference name, IEEE, 2011.

[14] Gamal A.Ebrahim”a VOIP spam reduction framework”In conference name, IEEE, 2013.

[15] Kentaroh Toyoda, IwaoSasase”SPIT callers detection with unsuperwised random forests classifier”In conference name, IEEE, 2013.

[16] NoppawatChaisamran,TaoukiYoukiKadobayashi, SuguruYamaguchi”Trust based SPIT detection by using call duration and social reliability”In conference name, IEEE, 2013.

[17] Urjasheeshaw, Bobby sharma “A survey paper on voice over Internet protocol (VOIP)” In International journal of computer application, April 2016.