Suresh Gyan Vihar University,
Jaipur International Journal of Converging Technologies and Management (IJCTM)
Volume 1, Issue 2, 2015
ISSN : 2455-7528

Fuzzy driven approach for spam filter to avoid unregistered calls

Rishi Kant Shukla [M. Tech IC,] Dr. Savita Shiwani [AssociateProfessor]
Department of Information Technology
Suresh Gyanvihar University,
Jaipur, Rajasthan, India
rishishuklark@gmail.com, Savita.Shivani@mygyanvihar.com

Abstract: Spam call was not a big problem, because VOIP telephone services were not widely used previously. However experts expected that this technology would become common over the next several years.
VOIP stands for Voice over Internet Protocol or in common terms it known as phone service over the Internet. Having a reasonable quality of Internet connection we may get phone service delivered via our Internet connection instead of from our local phone service provider company. Due to offering lower rates & increased functionality than traditional phone companies some people use VOIP in addition to their PSTN phones. With rapidly growth of VOIP telephony number of VoIP security and quality issues generated like Interception of calls, theft of service, call tampering, spamming etc. Spamming is going to become a serious issue in these years because every VoIP account associated with an IP address which leads to spammer to send their voicemail message to thousands of IP addresses & voicemail get choked and number of viruses, spyware also come along with them, which reduce the call quality of a VoIP system or may be crash the VoIP servers by eating the bandwidth.

In fact there is no any ideal & real-time solution that can be able to remove spam calls from a pool of VoIP calls. In this paper, I propose a real time algorithm to remove Spam calls on the basis of Fuzzy RTP media parameters checking system, Fuzzy MOS value checking system, Turing test and information about phone calls. At different stages of system checking, the stage may reject the spam calls after testing & verification of VoIP call. The results obtained that shows the algorithm is able to track and estimate VoIP System performance in real-time. This algorithm could be embedded in VoIP systems to allow rejection of VoIP spam calls in real-time.

1. Introduction

VoIP stand for Transmission of telephony services via use of IP infrastructure is a part of internet telephony. Internet telephony makes easy some things that are difficult to impossible with traditional phone networks and provides all telephony services like SMS, voice calling, voice mailing and fax etc. In VoIP technology, the voice signal is first segmented into frames, which are then stored in data packets, and lastly transported over IP network using voice communication protocol like H.3231 or the Session Initiation Protocol (SIP). As the VoIP systems become more popular, VoIP is gaining acceptance and becoming one of the main way of communication technology due to this the security in VoIP become a major issue. A large number of threats such as call tampering, toll fraud by phishing over VoIP and Man-in the middle attacks are the causes of SPIT calls.

Checking of spam emails is mature field and there are some similarities to our problem. In both problems domains, users can provide information & feedback about individual mail or call. But VoIP is a real time process so the detection should be also in real time. In this paper I proposed a system which contain few stages, each stage contain some basic rules, to check the originated call is a spam call or not. I also proposed two fuzzy interference systems with some parameters like DTMF detection ratio, clipping ratio front & back, wideband noise, hangover duration average and mean opinion score both audio & IP based to check the all condition, whether a call is spam or not.

Suresh Gyan Vihar University,
Jaipur International Journal of Converging Technologies and Management (IJCTM)
Volume 1, Issue 2, 2015
ISSN : 2455-7528

We evaluate the parameters by comparing the originated VoIP call stats with the common VoIP service quality thresholds reference chart.

In this paper I also focused on Turing tests, these tests are techniques whereby the sender of the message is given some kind of puzzle or challenge, which only a human can understand & can give answers. Turing tests rely on video or audio puzzles. These tests are also known as captchas (Completely Automated Public Turing test to tell Computers and Humans part). If the puzzle is answered correctly, the sender is placed on the user's white list. Turing tests can be applied to call spam as well, although not directly, because call spam does not usually involve the transfer of images and other content that can be used to verify that a human is on the other end. If most of the calls are voice, the technique needs to be adapted to voice. This is not that difficult to do. Here is how it could be done. User A calls user B and is not on user B's white or black list. User A is transferred to an Interactive Voice Response (IVR) system. The IVR system tells the user that they are going to hear a series of numbers (say 5 of them), and that they have to enter those numbers on the keypad. The IVR system reads out the numbers while background music is playing, making it difficult for an automated speech recognition system to be applied to the media. The user then enters the numbers on their keypad. If they are entered correctly, the user is added to the white list.

So we may say that it is a complete ideal package with number of stages to remove the spam call in a real time VoIP system.

1.1. Theoretical Background

Spam, defined as the transmission of bulk unsolicited email, has been a plague on the Internet email system. Many solutions have been documented and deployed to counter the problem. None of these solutions is ideal. However, one thing is clear: the spam problem would be much less significant had solutions been deployed ubiquitously before the problem became widespread.

Problem Definition: The spam problem in email is well understood, and we make no attempt to further elaborate on it here. The question, however, is what the meaning of spam when applied to SIP is? Since SIP covers a broad range of functionality, there appear to be three related but different manifestations:

Call Spam: This type of spam is defined as a bulk unsolicited set of session initiation attempts (i.e., INVITE requests), attempting to establish a voice, video, instant messaging [1], or other type of communications session. If the user should answer, the spammer proceeds to relay their message over the real-time media. This is the classic telemarketer spam, applied to SIP. This is often called Spam over IP Telephony, or SPIT.

IM Spam: This type of spam is similar to email. It is defined as a bulk unsolicited set of instant messages, whose content contains the message that the spammer is seeking to convey. IM spam is most naturally sent using the SIP MESSAGE [3] request. However, any other request that causes content to automatically appear on the user's display will also suffice. That might include INVITE requests with large Subject headers (since the Subject is sometimes rendered to the user), or INVITE requests with text or HTML bodies. This is often called Spam over Instant Messaging, or SPIM.

Call Spam: Will call spam occur? That is an important question to answer. Clearly, it does occur in the existing telephone network, in the form of telemarketer calls. Although these calls are annoying, they do not arrive in the same kind of volume as email spam. The difference is cost; it costs more for the spammer to make a phone call than it does to send email. This cost manifests itself in terms of the cost for systems that can perform telemarketer call, and in cost per call. Both of these costs are substantially reduced by SIP. A SIP call spam application is easy to write. It is just a SIP User Agent that initiates, in parallel, a large number of calls. If a call connects, the spam application generates an ACK and proceeds to play out a recorded announcement, and then it terminates the call. This kind of application can be built entirely in software, using readily available (and indeed, free) off-the-shelf software components. It can run on a low-end PC and requires no special expertise to execute. The cost per call is also substantially reduced. A normal residential phone line allows only one call to be placed at a time. If additional lines are required, a user must purchase more expensive connectivity. Typically, a T1 or T3 would be required for a large- volume telemarketing service. That kind of access is very expensive and well beyond the reach of an average

Suresh Gyan Vihar University,
Jaipur International Journal of Converging Technologies and Management (IJCTM)
Volume 1, Issue 2, 2015
ISSN : 2455-7528

user. A T1 line is approximately US $250 per month, and about 1.5 cents per minute for calls. T1 lines used only for outbound calls (such as in this case) there are two aspects to the capacity: the call attempt rate, and the number of simultaneous successful calls that can be in progress. A T1 would allow a spammer, at most, 24 simultaneous calls, and assuming about 10 seconds for each call attempt, about 2.4 call attempts per second. At high-volume calling, the per-minute rates far exceed the flat monthly fee for the T1. The result is a cost of 250,000 micro cents for each successful spam delivery, assuming 10 seconds of content. With SIP, this cost is much reduced. Consider a spammer using a typical broadband Internet connection that provides 500 Kbps of upstream bandwidth. Initiating a call requires just a single INVITE message. Assuming, for simplicity's sake, that this is 1 KB, a 500 Kbps upstream DSL or cable modem connection will allow about 62 call attempts per second. A successful call requires enough bandwidth to transmit a message to the receiver. Assuming a low compression codec (say, G.723.1 at 5.3 Kbps), this requires approximately 16 Kbps after RTP, UDP, and IP overheads. With 500 Kbps upstream bandwidth, this means as many as 31 simultaneous calls can be in progress. With 10 seconds of content per call, that allows for 3.1 successful call attempts per second. If broadband access is around $50/month, the cost per successful voice spam is about 6.22 micro cents each.

This assumes that calls can be made 24 hours a day, 30 days a month, which may or may not be the case. These figures indicate that SIP call spam is roughly four orders of magnitude cheaper to send than traditional circuit-based telemarketer calls.

This low cost is certainly going to be very attractive to spammers. Indeed, many spammers utilize computational and bandwidth resources provided by others, by infecting their machines with viruses that turn them into "zombies" that can be used to generate spam. This can reduce the cost of call spam to nearly zero.

1.2. Related Works

In 2006 Rainer Baumann, Stephane Cavin and Stefan Schmid in University of Berne recommended that VoIP growth and its security issues are rapidly evolving as discussion is going with many known researchers. As we seen many known system like Google talk, MSN, Skype, Yahoo etc. provide services to registered members that they can interconnect to each other but the user first have to be registered for using application this application is being used by world-wide system As the technology is evolving many new threats / viruses also emerging such as SPIT.

In 2007 S. Tartarelli, M. Brunner, T. Ewald, M. Stiemerling, J. Quittek, S. Niccolini, , from Europe Ltd., Kurfürsten-Anlage 36, 6915 Heidelberg, Germany, As they all mentioned email spam issue, this test is based on fuzzy logic which will compare SPIT calls with normal calls based on human communication pattern so several advantages are there comparing with other methods the test feasibility is good. By using this prototype application a VoIP SEAL is being given by modular VoIP security system.

In 2007 Nick Feamster, Santosh Vempala Anirudh Ramachandran, from College of Computing, Atlanta, GA 30332, USA presented Spam Tracker, in which a technique was used for spam filtering system & it was called behavioral blacklisting this technique classify emails of sender user to reveal its identity from their sending tracks As these trackers were not based on the new or fresh IP address Because these are based on patterns of the sender that is invariant in nature. These application use fast clustering algorithms that give reaction in sending pattern Spam Tracker has ability to evaluate or classify spammers.

In 2008 Ying-You, Zhao Hong, He Guang-Yu, Wen China has also participated in resolving SPIT Spam over Internet Telephony security risk in the network of convergence ALL-IP. In this many prevention & detection methods are used based on feedback judgment. In this method user is participated with trust & reputation which can make feedback simple effective and lossless by direct & indirect sense. So this improved algorithm comprises the distribution behavior of SPIT characteristics which also reflect its relation and its results. The new algorithm comprises of trust & reputation. By using this technique of trust & reputation which make detailed evaluation of the SPIT. This experiment shows greater accuracy & better Sensitivity of the methods which specify the efficiency of the detection and prevention.

In 2009 Yan Bai1, Xiao Su2 and Bharat Bhargava3

proposed that unlike detection and filtering of e-mail spam, countermeasures against SPIT face great challenges on how to identify and filter SPIT in real time. In this paper, a user-behavior aware anti-SPIT technique implemented at the router level for detecting and filtering SPIT is proposed. The rationale for the technique is that voice spammers behave significantly different from legitimate callers because of their revenue-driven motivations. The technique defines and combines three features developed from user behavior analyses to detect and filter spam calls. Compared to existing SPIT defending techniques, it is simple, fast and effective. Other advantages of our approach are that it is applicable for detecting and filtering both machine-initiated and human-initiated spam calls, better protects VoIP calls against Sybil attacks and spammer behavior changes.

In 2013, Ji-Yeon Kim1, Hyung-Jong Kim2 proposed that VoIP (Voice over Internet Protocol) services can be abused by spammers who send out commercial messages in bulk due to their cost saving effects. However, an effort to prevent spam has hardly been made in implementing VoIP system, so that a spam reporting system that collects various types of VoIP spam and makes use of them to impose legal sanctions or to improve spam filtering techniques has not yet been developed. In this paper, we propose a VoIP spam reporting system by extending an existing spam reporting system of mobile phones. We design a message format for reporting VoIP spam by analyzing CDR (Call Detailed Records) that can be obtained from VoIP devices, and propose various paths which connect VoIP phones to spam reporting servers. In addition, we design the system modules and elicit their functional requirements of hardware and software.

2. The Proposed Procedure

In this section I proposed few steps to remove the Spam calls from a VoIP system, while rejecting the Spam calls, I mainly focused on some parameters like, call identity, callee identity, silent duration in RTP media streaming, black listing and white listing. I also considered some basic components of SDRTP streaming like DTMF detection ratio, back & front clipping ratio, wide band noise, hangover duration average and bit error ratio. Which helped us to compute the standard situation of a VoIP call, should be reject or not. I proposed all above parameters in fuzzy interference system to compute the situation of point at which a normal VoIP call will consider as Spam call. There is a short description about the parameters which I used in proposed fuzzy inference system.

1. **DTMF detection ratio:** Dual-tone multi-frequency signaling (DTMF) is used for telecommunication signaling over analog telephone lines in the voice-frequency band between telephone handsets and other communications devices and the switching center. Its ratio is the percentage of DTMF digits (0, 1, 2, 3 …., #, etc.) properly transmitted.

2. **Back, front & in-between clipping ratio:** Clipping is defined as the duration of lost speech samples. % of speech subjected to back end clipping, front end clipping and in-between clipping, generally known as their ratio.

3. **Wide Band Noise:** Noise level on a silent wideband channel.

4. **Hangover duration average:** Average VAD hang-over time (Duration of sound not transmitted due to VAD delay).

5. **Mean opinion score:** A common subjective benchmark for quantifying the performance of the speech codec is the mean opinion score (MOS). MOS tests are given to a group of listeners. Because voice quality and sound in general are subjective to listeners, it is important to get a wide range of listeners and sample material when conducting a MOS test. The listeners give each sample of speech material a rating of 1 (bad) to 5 (excellent). The scores are then averaged to get the mean opinion score.

Here I proposed different parameters which estimate RTP media content and on the basis of those I made my system. Therefore, we have taken parameters from real time system so the input parameters that we get from a standard are:

1. Hangover duration.

2. DTMF detection ratio.

3. Clipping Ratio-Front.

4. Clipping Ratio-Back.

Suresh Gyan Vihar University,
Jaipur International Journal of Converging Technologies and Management (IJCTM)
Volume 1, Issue 2, 2015
ISSN : 2455-7528

5. Wideband Noise

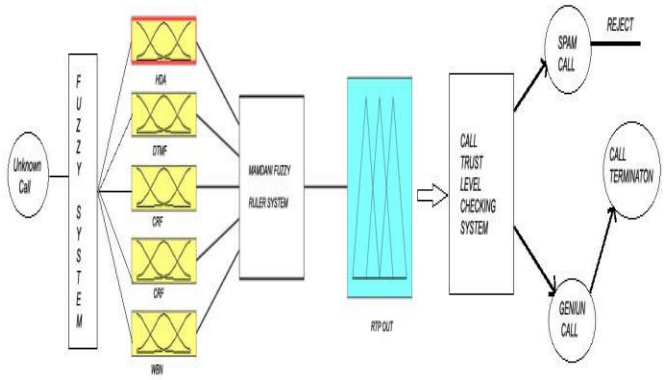

Figure 1:-Fuzzy interference system removes spam call in VoIP

To achieve a real-time low computationally complex algorithm, we have to drive output membership functions of each parameter using fuzzy interference system showing the effect on the output.

Table no. 1 shows the fuzzy sets associated with the input parameters and effect on proposed.

So we have defined two output membership functions of which will give an estimate of the delay content of voice traffic can be described by the following equations.

Membership functions for Hangover duration detection Ratio

The "Good Hangover duration average" membership function of fuzzy set

$$\mu_{Good\_Hda}(x)=\begin{cases}1, & for\ 0<x<200\\ \dfrac{250-x}{50}, & for\ 200\le x\le 250\\ 0, & for\ x>250\end{cases}$$

The "Bad Hangover duration average" membership function of fuzzy set

$$\mu_{Bad\_Hda}(x)=\begin{cases}1, & for\ 350<x<1000\\ \dfrac{350-x}{100}, & for\ 250\le x\le 350\\ 0, & for\ x<250\end{cases}$$

This approach defines the input membership functions which are based on standards that we have got from Mincom matrix chart, after this we will define membership functions on fuzzy interference system by using the output algorithm after then we define the rules and regulation on which this theorem is based

In the next paragraph I describe the proposed a set of fuzzy rules, defuzzification and operations in fuzzy inference system.

The fuzzy membership functions collectively with the fuzzy rules are the chief fundamentals that used triangular method for the proposed fuzzy inference system. Now we would explain few fuzzy rules in brief for the fuzzy inference input/ output variables for which we have define some membership functions which are being used in our proposed algorithm

1. If (hda is Ghda) and (DTMF is Gdtmf) and (CRB is Gcrb) and (CRF is Gcrf) and (WBN is Gwbn) then (RTP is BadRTP) (1)
2. If (hda is Bhda) and (DTMF is Gdtmf) and (CRB is Gcrb) and (CRF is Bcrf) and (WBN is Bwbn) then (RTP is GoodRTP) (1)
3. If (hda is Bhda) and (DTMF is Gdtmf) and (CRB is Bcrb) and (CRF is Bcrf) and (WBN is Gwbn) then (RTP is GoodRTP) (1)
4. If (hda is Ghda) and (DTMF is Bdtmf) and (CRB is Bcrb) and (CRF is Bcrf) and (WBN is Bwbn) then (RTP is GoodRTP) (1)
5. If (hda is Ghda) and (DTMF is Gdtmf) and (CRB is Bcrb) and (CRF is Bcrf) and (WBN is Gwbn) then (RTP is BadRTP) (1)
6. If (hda is Ghda) and (DTMF is Gdtmf) and (CRB is Bcrb) and (CRF is Gcrf) and (WBN is Gwbn) then (RTP is BadRTP) (1)
7. If (hda is Bhda) and (DTMF is Gdtmf) and (CRB is Gcrb) and (CRF is Gcrf) and (WBN is Gwbn) then (RTP is BadRTP) (1)
8. If (hda is Bhda) and (DTMF is Gdtmf) and (CRB is Bcrb) and (CRF is Bcrf) and (WBN is Bwbn) then (RTP is GoodRTP) (1)

We have used MATLAB software and in which we are using fuzzy logic toolbox to implement our proposed algorithm for this we have taken 15 calls and on that basis we would evaluate our result. The version of software we are using MATLAB 2009a version in which we can feed the value using diverse fuzzy inference systems at a time. So the input/output variables and fuzzy rules are same for each membership functions but we have define different membership functions for each case As we have taken 15 calls based on these we will evaluate voice traffic.

As there are so many parameters that can be used to define RTP media content .and we have define three membership function using (TrFn) triangular membership that has a positive/ negative slope As a result we have derived the following membership functions for the fuzzy sets.

Membership functions for DTMF detection Ratio:

The "Good DTMF detection ration" membership function of fuzzy set

Suresh Gyan Vihar University,
Jaipur International Journal of Converging Technologies and Management (IJCTM)
Volume 1, Issue 2, 2015
ISSN : 2455-7528

$$\mu_{Good\_Dtmf}(x)=\begin{cases}1, & for\ x\geq 100\\ \dfrac{100-x}{10}, & for\ 90\leq x\leq 100\\ 0, & for\ x<90\end{cases}$$

The "BAD DTMF detection ration" membership function of fuzzy set

$$\mu_{Bad\_Dtmf}(x)=\begin{cases}1, & for\ 0<x<70\\ \dfrac{90-x}{20}, & for\ 70\leq x\leq 90\\ 0, & for\ x>90\end{cases}$$

Membership functions for clipping Ratio front:

The "Good clipping ratio front" membership function of fuzzy set

$$\mu_{Good\_CLF}(x)=\begin{cases}1, & for\ 0<x\leq 1\\ \dfrac{2-x}{1}, & for\ 2<x<1\\ 0, & for\ x>2\end{cases}$$

The "Bad clipping ratio front" membership function of fuzzy set

$$\mu_{Bad\_CLF}(x)=\begin{cases}1, & for\ 4<x<5\\ \dfrac{4-x}{2}, & for\ 2<x<4\\ 0, & for\ x<2\end{cases}$$

Membership functions for clipping Ratio Back:

The "Good clipping ratio back" membership function of fuzzy set

$$\mu_{Good\_CLB}(x)=\begin{cases}1, & for\ 0<x\leq 1\\ \dfrac{2-x}{1}, & for\ 2<x<1\\ 0, & for\ x>2\end{cases}$$

The "Bad clipping ratio back" membership function of fuzzy set

$$\mu_{Bad\_CLB}(x)=\begin{cases}1, & for\ 4<x<5\\ \dfrac{4-x}{2}, & for\ 2<x<4\\ 0, & for\ x<2\end{cases}$$

Membership functions for Wide Band Noise:

The "Good wide band noise" membership function of fuzzy set

$$\mu_{Good\_WBN}(x)=\begin{cases}1, & for\ 0\leq x\leq 32\\ \dfrac{40-x}{8}, & for\ 32<x<40\\ 0, & for\ x>40\end{cases}$$

The "Bad wide band noise" membership function of fuzzy set $\mu_{Bad\_WBN}(x)=\begin{cases}1, & for\ 57<x<90\\ \dfrac{57-x}{17}, & for\ 40<x<57\\ 0, & for\ x<40\end{cases}$

3. Performance Evaluation

Now we estimate the performance of our proposed real-time spam checking approach, numerous simulations were performed using MATLAB for a one–to–one VoIP voice call situation. So in this section, we will present a detailed explanation of the estimate process and results obtained.

In this algorithm we have taken 15 calls with different levels of call parameters. All these calls were all earlier generated during a live VoIP call and recorded in PCM format. After that we have taken their measurements and analyzed these calls after then we have used these calls as an input to our fuzzy algorithm. Now we take parameter which we have define in earlier section we take those recorded call parameters measurements that were the Hangover duration time, DTMF detection ratio, Clipping Ratio-Front, Clipping Ratio-Back and Wideband Noise. And the output is evaluated from above parameter that is RTP OUT.

S.No.	HAD	DTMF	CRF	CRB	WBN	RTPOUT
1	210	80	2.5	2.8	43	0.7739
2	217	87	2.5	3.5	43	0.7708

Suresh Gyan Vihar University,
Jaipur International Journal of Converging Technologies and Management (IJCTM)
Volume 1, Issue 2, 2015
ISSN : 2455-7528

3	218	88	2.5	3.6	43	0.7648
4	219	89	2.5	3.7	43	0.7589
5	405	108	0.5	0.8	23	0.1633
6	406	109	1.5	1.8	24	0.2234
7	407	110	2.5	2.8	25	0.7823
8	408	111	3.5	3.8	26	0.8278
9	409	112	4.5	4.8	27	0.8367
10	410	113	5.5	5.8	28	0.5
11	411	114	1.333	1.32	29	0.1778
12	251	115	1.5	1	30	0.245
13	252	60	1.89	1.99	29	0.5
14	251	115	1.5	1	30	0.245
15	202	115	1.5	1	30	0.1918

Table1. Average reading of 15 VoIP Calls.

As shown from the table we have recorded the 15 VoIP call and the parameter that are used to show the RTP type in VoIP call in VoIP network the output shown from these parameter that is Real time media changing according to the different value of the HAD, DTMF, CRF, CRB, WBN. According to the different value of the above parameter we can evaluate the RTP media type of VoIP call in VoIP network to identify the characteristics of a VoIP calls that differentiate a spam call and a VoIP call characteristics.

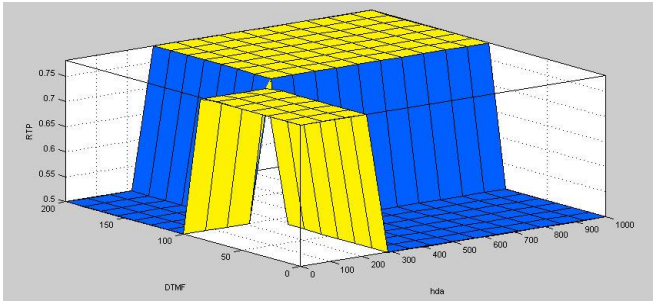

Figure 2 :-MATLAB surface view for HAD, DTMF and RTP

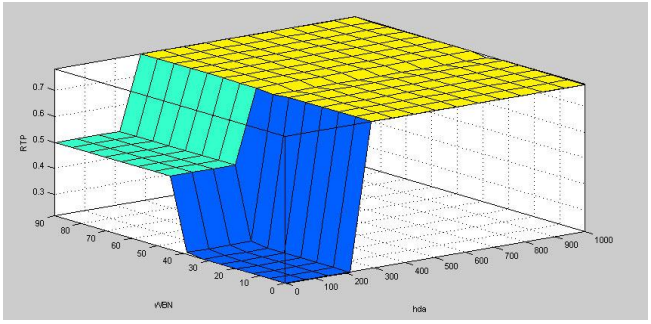

Figure 3 shows a 3-D view of the RTP media type content, showing MATLAB surface of HDA and WBN and their relationship with RTP media type. We can conclude from these outputs by comparing RTP OUT with the distrust level of call that is base on the security and social science theory of Ray and chakra borty 2004 and Hepburn and Wright 2003. As per this theory trust is traditionally used in solving the problem of authentication in application level like ad-hoc & peer to peer network systems but the social notation of trust can we used surmising the spam behavior of voice calls. So we may say that trust of incoming new unwanted call is based on trust of caller capability, honesty, and reliability in making logical (justified) calls to callee. It means trust level of a call may be base on call participants which may also derived from callers past behavior. So here I grouped the calls in white, grey and black based on past experience, current needs and distrust then assigned some ranges of distrust level like for white (0-0.01), black (.01-.99) and black (.99-1.0).

Now in last step of evaluation I have two parameters to check that an unregistered call is spam or not, first is RTP_OUT & second is distrust level. On the basis of this by making some policies we will filter call as spam call or a genuine call forward for termination.

We can conclude from these results that the proposed algorithm correctly identifies and remove the spam call from the unregistered calls to terminate in VoIP switch. Which make the VoIP calls more secure and efficient for bandwidth utilization.

4. Conclusions &Future Aspects

The results of our simulations are analyzed and discussed in this section. The results are analyzed and discussed in taking 15 different voice calls for evaluating voice traffic. This effort presented an algorithm which is a main element for evaluating voice traffic using real time system algorithm in that we identifies and remove unregistered VoIP calls in real time system by taking live calls.

Simulations using fuzzy logic in MATLAB software also good result good result with low computational complexity. This algorithm provides frequents result on the network and evaluate voice traffic with respect RTP content this all can be done without taking reference signal and easily control the voice traffic.

As we know that in today's environment, the technology and problems related to these technologies are continuously changing so using real time fuzzy approaches we can easily update of security system as per the current scenario.

The future work for this section is that in future we work on more real time system algorithm so that we frequently evaluate the results and on that we achieve maximum genuine VoIP calls to increase the efficiency of a VoIP network and also give better VoIP quality calls to our users.

REFERENCES

1. Ross, T. (2004) Fuzzy Logic sets with Engineering Application Sense willey (2004)
2. Periakarruppan, G.; Azhar, H.; A.L.Y.; Rashid, A., (2006) Packet Based Echo Cancellation for Voice Over Internet Protocol Simulated with Variable Amount of Network Delay Time,. 2006 IEEE Region 10 Conference, pp 1 to 4.
3. Lingfen Sun and Emmanuel C. Ifeachor (2006) Perceived Speech Quality Prediction fsor Voice over IP-based Networks, Department of Electronics' Communication and Electronic Engg., University of Plymouth, Plymouth PL4 .
4. In 2006 Rainer Baumann, Stephane Cavin and Stefan Schmid in University of Berne, recommended that VoIP world is evolving rapidly and its security issues are well discussed among researchers.
5. In 2007 S. Tartarelli, J. Quittek, S. Niccolini, M. Stiemerling, M. Brunner, T. Ewald from NEC Europe Ltd., Kurfürsten-Anlage 36, 6915 Heidelberg, Germany, described about the email spam problem, which could evolve in the next years towards a problem affecting the next contemporary's telephone system based on IP.
6. Sociao-Technical defense against spamming PRAKASH KOLAN and RAM DANTU University of north Texas, Denton, Texas, ACM Transaction on Autonomous and Adaptive System, Vol.2, No.1, Article 2, Publication date: March 2007.
7. A. Khorsi, "An Overview of Content-based Spam Filtering Techniques", Informatica, vol. 31, no. 3, October 2007, pp 269-277.
8. Y. Rebahi, S. Ehlert, and A. Bergmann, "A spit detection mechanism based on audio analysis," in Proceedings of 4th International Mobile Multimedia Communications Conference MobiMedia 2008: July 7-8, 2008, Oulu, Finland. ICST; ACM, 2008.
9. Wai-Yip Chan and Falk, T.H. and. (2008) Hybrid Sig-nal-and-Link-Parametric Speech Quality Measurement for VoIP Communications, Speech, Audio, and Language Processing, vol.16, no.8, pp.1579-89.
10. In 2008 Ying-You, Wen and Zhao Hong, The Software Center of Northeastern University, Shen Yang, China anticipated to resolve the SPIT Spam over Internet Telephony security risk in the ALL-IP convergence network.
11. SPIT detection and prevention Method in VoIP environment, He Guang-Yu, Wen Ying-You, and Zhao Hong, Software center of N, Shen Yang, China 2008 IEEE.
12. C. Porschmann and H. Knospe, "Spectral analysis of audio signals for the identification of spam over IP telephony," in Proceedings of the NAG/DAGA 2009. NAG/DAGA International Conference on Acoustics, 23.-26. March 2009, Rotterdam, Nederland, 2009.
13. Petri, D. and Paglierani, P. (2009) Uncertainty valuation of Objective Speech Quality Measurement in VoIP Systems, Measurement and Instrumentation , vol.58, no.1, pp.46-47.
14. A fuzzy logic classification of incoming packet for a VoIP, Suardinata, Kamalrulnizam, University Teknologi Malaysia, 81310 skudia, Johor, Malasiya, STMIK Indonesia Padang, Indonesia 2010.
15. Ren, Jiuchun;, WeiChao ,ChongMing; Mao, Dilin, Zhang (2010) Enhancement to E-Model on standard deviation of packet delay,2010 3rd International Conference, vol. 23,24,25, pp.256-259.
16. Ditech Networks. Echo Basics Tutorial including echo cancellers and echo's effect on QoS" (2010) http://www.dite chnetworks.org/learning Center/echoBasics.html.
17. Adaptive Digital Technologies, (2010) The Echo "Pheno-menon", Solutions and Causes http://www.adaptivedigital.com/product/echo_cancel/echo_explain.htm.

18. Dr. Sarabjeet Singh, Harjit Pal Singh Dr.Jasvir Singh, (2010) Computer Modeling & Performance study of VoIP under Different planned Conditions, Computer Engg. And Applications (ICCEA), 2010 Second International Conference, vol.1, pp 612 – 15

19. Thompson, R. and Ngamwongwattana, B. (2010) Sync &assess One-Way Delay without Clock Synchronization-Instrumentation and Measurement, vol. 59, pp 1319 – 26.

20. Chien-Chung Shen and Justin Yackoski, (2010) Managing End-to-End Delay for VoIP Calls in Multi-Hop Wireless N/w s, IEEE Comm. Society subject matter experts for publication in the IEEE INFOCOM 2010 proceedings.

21. Fuzzy Modeling of a network denial of service attack phenomenon, IHEKWEBABA. OGECHI, CHUKWUGOZIEM, INYIAMA H.C. International Journal of engineering and technology (IJET), issn: 0975-4024 Vol5 No-2 Apr-May 2013.

Suresh Gyan Vihar University,
Jaipur International Journal of Converging Technologies and Management (IJCTM)
Volume 1, Issue 2, 2015
ISSN : 2455-7528