ISSN: 0976-3104
SPECIAL ISSUE: (Emerging Technologies in Networking and Security (ETNS)
Banu and Mehata

THE IIOAB JOURNAL

ARTICLE OPEN ACCESS

VOIP PERFORMANCE ENHANCEMENT THROUGH SPIT DETECTION AND BLOCKING

Saira Banu*, K.M. Mehata
**Assistant Professor (Senior Grade), B.S.Abdur Rahman University, Chennai. INDIA*
Dean(SCISM), B.S.Abdur Rahman University, Chennai, INDIA

ABSTRACT

SPIT will burst as a major threat in the coming future because of the exponential growth of the VOIP users. spam callers like advertiser, telemarketers, prank callers make use of this VOIP for generating the bulk unwanted calls and messages. SPIT is hard to perceive than the mail spam. Injection of spam caller consumes more bandwidth and congest the network This paper proposes a pre acceptance method to detect the Voice spam based on the call intervals between the call and the online network reputation to identify the legitimate and non-legitimate caller. Realistic simulation results prove that our approaches are effective in discriminating the spammer from legitimate user.

Published on: 2nd -December-2016

KEY WORDS

VoIP, SPIT, CDR, Call interval, Pre acceptance.

***Corresponding author: Email:** saira.atham@gmail.com; **Tel.:** +91 9444420675

INTRODUCTION

VoIP is used for data transition on IP based networks. With the growth of broadband connectivity, Voice over Internet Telephony is widely used for voice communication. The VoIP technique converts the analog signal to digital signal by using specific codecs. VoIP can support different types of data such as image, voice, video, and fax. The different services provided by VoIP are remote conference, call baring and call forwarding.

The important threats in VoIP network is known as SPIT (Spam over Internet Telephony). Advertiser and prank callers are using VoIP for sending unsolicited bulk calls like spam in emails. The spam detection in VoIP is more difficult than the detection of email spam because, the callee is directly connected by the incoming call. The Spam call makes irritation to VoIP users. For example a spam email that arrives to the inbox at 3a.m. will not disturb the particular user. But the spam call at 3a.m. will be irritated for the user. SPIT is the cost effectiveness for the spam callers. In VoIP network SPIT is most popular because of cheap hardware cost, low call fee, and there is no boundary for international calls [13].True caller is an android app that identifies the caller and it also identifies the spammer if the number is already in the spam list. This spam list is manages by getting feedback from the caller.

In this paper we use the call intervals between calls and the online shopping pattern of the caller is taken for identifying the spam caller. The online reputation is based on the online shopping pattern of the caller. This method is used to find the spam callers without analyzing the data and without getting feedback from the user.

The CDR (Call Detail Record) contains the information of the call duration, call rate of the VoIP users. The details of call rate and call duration is used to generate the social network graph. The social network graph is used to find direct trust value. Direct trust between caller and the callee is the combination of the amount of time both users engaged in talking and the number of reciprocal calls between them, and number of unique callees of the caller [1].This direct trust value is taken as the input for finding global reputation score. The global reputation value will be compared with the threshold value to identify the behavior of user. If the global reputation value is lesser than the threshold value then the caller is identified as the non legitimate caller, else he/she is identifying as legitimate caller. After finding the spam call, the information about the spam call will shared with other VoIP users to know whether they have interested to attend those calls or not interest. If they are not interest, in future those spam call will not establish through SIP (Session Initiation Protocol).

Fig: 1.True caller app for identifying the spam call

The major works are:

- Getting the caller-callee information from CDR.
- The call detail record has the complete information about the staring time, ending time, call duration , call type and the call routing information of each call.
- The call intervals between the calls can be computed using the starting time of the calls.
- The details of the incoming and outgoing sms are recorded in the call detail record.
- One Time Password(OTP) is a type of sms used for authentication purpose during online shopping, online money transaction etc.
- This OTP registered in the CDR is used for calculating the online network reputation of the caller.
- The call intervals between calls and the online network reputation together used to differentiate the spam caller s from legitimate caller
- This information is used to block the spam calls before the call is setup using the session initiation protocol.
- This scenario is simulated in a WiMax environment and the bandwidth consumed by the spammer for a single day is calculated .
- Thus SPIT detection and blocking will enhance the performance of the VOIP.

BIGDATA

A. IP Telephony

IP telephony is a technology, which compresses the telephone voice signal into data packets for transmission over the Internet. Protocols are used in carrying the voice signals over the IP networks are referred to as Voice over IP (VoIP).
IP telephony moves away from the traditional circuit switched voice networks like Public Switched Telephone Networks (PSTN's) to a packet switched one where IP packets containing voice data are sent over the network.

The advantages of IP telephony over traditional telephony are lower infrastructure costs and lower costs per call (or even free calls). IP telephony comprises, independent of the protocols used, a multimedia plane and a signalling plane. The signalling plane is used for transporting the signalling information, during call setup. The media transport plane is used to carry voice data packets between IP telephony components [14].

B. VoIP (Voice over Internet Telephony)

Voice over IP is a technology for transmitting voice packets on the existing IP network between two communicating parties which are connected to the Internet. Unlike PSTN networks, an IP network is packet

switched. In PSTN networks, when the calling party calls the called party, there exist a physical between the two parties. Then the parties can communicate with each other, and the circuit is reserved until they finish their communication.

In an IP network, all communication is carried out using IP packets. When a calling party communicates with a called party, the analog signals converted into digital signal, encoded, and it is packed into an IP packet at the transmitting end and converted back to analog signals at the receiving end.

C. SIP (Session Initiation Protocol)

SIP, published as RFC 3261, is an application-layer protocol [14]. It can be used for creating, modifying and terminating sessions with one or more participants. The protocol which specifies a set of signalling messages for connection establishment and connection termination. It is used with other transport protocols like RTP (Real-time Transport Protocol), RTCP (Real time Control Protocol) for enabling voice-communication services between two parties. Requests are generated by the client and sent to the server. The server will process the requests and then sends back a response to the client.

SIP makes minimal assumptions about the transport protocol and this protocol provides reliability and it does not depend on TCP for reliability. Session Initiation Protocol depends on the Session Description Protocol to carry out the negotiation for codec identification. SIP supports for session descriptions that allow the participants to agree on a set of compatible media types. The services provided by SIP include:

- Location of user: Determination of the end system used for communication.
- Capabilities of user: Determination of the media and parameters to be used
- Call handling: Used for the transfer and termination of calls
- Call Setup: Establishing and ringing call parameters at both the calling and the called party

FREQUENT SUBGRAPH MINING

The caller generates a call request to a callee through the SIP proxy server. The server checks for the registered user with the domain SIP register. After identifying the caller as a registered user the proxy server uses the SIP location server. If the callee is in the same domain as the calling party, then the proxy server forwards the call directly to the callee's end device.

The SIP messages are used for communicating between the client and the SIP server shown in **Figure- 2** are discussed below:

- INVITE used for inviting a user to a call
- BYE message used for terminating a connection between the two end points
- ACK is used for reliable exchange of invitation messages
- OPTIONS message used for getting information about the capabilities of call
- REGISTER gives the information about the location of a user to the SPIT registration server
- CANCEL message is used to terminating the sessions

LITERATURE SURVEY

Spam over Internet Telephony is a major problem for VoIP users. It affects the private life of VoIP customers and their correspondents.

Ricardo Morla et al, [1] proposed novel content independent, non-intrusive approaches based on caller trust and reputation to block spam callers in a VoIP network. This approach is based on interaction rate, call duration and caller out- degree distribution. It is used to establish a trust network between VoIP users and computes the global reputation of a caller across the network. Gamal A. Ebrahim [2] followed to reduce VoIP Spam by ranking VoIP callers based on a set of parameters. The parameters are caller's reputation, the feedbacks (if any) collected from the called party, and whether the callee responds the call or ignores the call. In Addition, a set of dummy directory numbers is introduced in the callee's domain and these numbers work as traps for certain kinds of VoIP spammers who try to guess the directory numbers in the domain of victim by dialling random directory number. Based on this the spam callers are identified.

Dirk Lentzen et al, [3] designed a system that combines with the advantages of signalling-based SPIT

ISSN: 0976-3104

prevention and audio content-based SPIT detection. This is achieved by calculating spectral audio fingerprints and detecting SPIT calls with identical or similar voice data. The result of the fingerprint comparison is used to generate black list entries. This system integrated into existing VoIP environments and SPIT filter systems. Kentaroh Toyoda et al, [4] proposed a multi-feature call pattern analysis with unsupervised Random Forests Classifier. It is one of the classification algorithms.

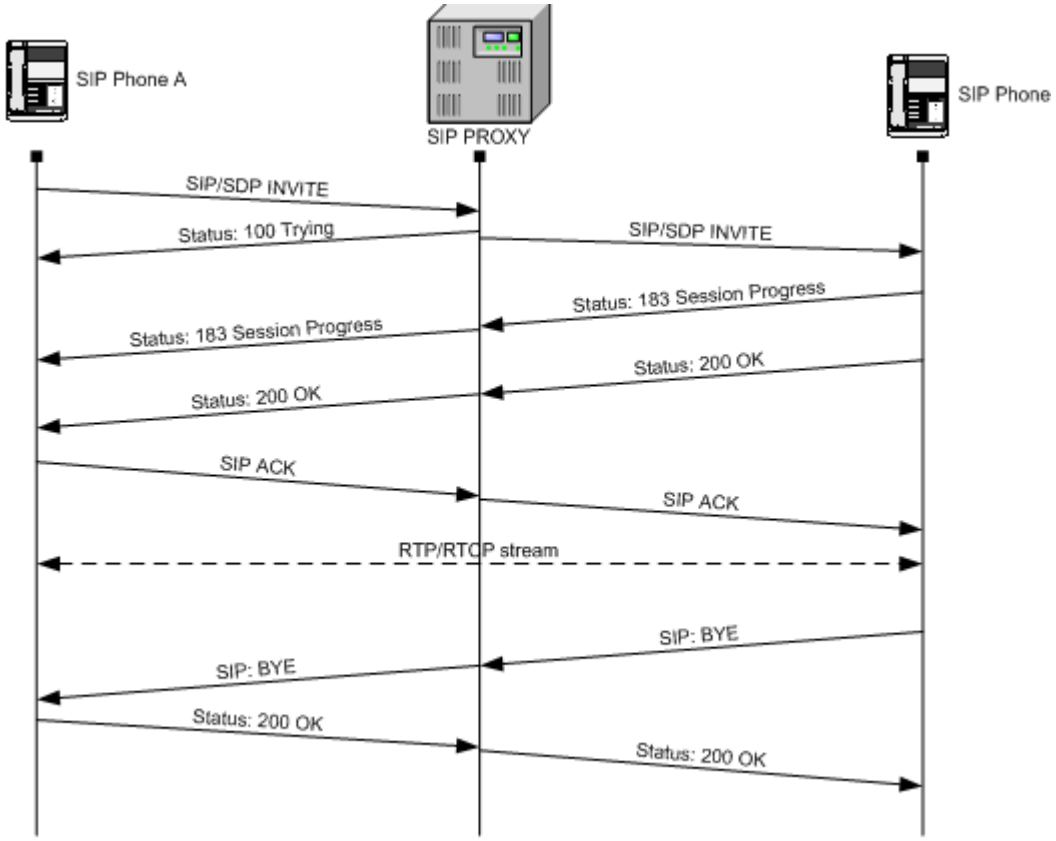

Fig: 2 . Basic SIP Messages

There are two features in Random Forests Classifier. That is BDR (Bi-Direction Ratio) and IOR (Incomings/Outgoings Ratio). BDR indicates the ratio of the intersection of Incomings and Outgoings to the number of Outgoings and IOR represents the ratio of Incomings to the union of Incomings and Outgoings. Based on this classifier the spammer is detected.

Yan Bai1 et al, [5] followed a user-behavior-aware anti-SPIT technique. It is implemented at the router level for detecting and filtering SPIT. Based upon this rationale technique voice spammers behave significantly different from legitimate callers because of their revenue-driven motivations. This technique defines and combines three features developed from user behavior analyses. This approach is applicable for detecting and filtering both machine-initiated and human-initiated spam calls. He Guang-Yu et al, **[6]** a detection and prevention method based on feedback judgment, the SPIT problem can be resolved. The improved inference algorithm embodies the characteristic of SPIT behavior and also it's reflects the weight relation of factors which influence the result. The incremental learning algorithm gives the Real-time trust and reputation. The algorithm integrates the trust with the reputation and it makes a comprehensive evaluation of the SPIT.

PROPOSED APPROACH

Call intervals method in VoIP users is a mechanism for detecting the SPIT (Spam over Internet Telephony) callers. The existing approaches are based on content analysis, user involvement, list based (white, black, gray) and reputation based . But Call interval method does not depends on above list. Call interval is the observation of the difference in time intervals between the consecutive calls of the caller. If the mean call intervals is lesser than the threshold value and if the online network reputation is also lesser than the minimum value then the caller is fully decided as a spam caller. The Wimax environment with the injected Spam caller is simulated for 9 hours and the consumed bandwidth is calculated. The performance of the WIiMax scenario is found to degrade when simulated with the spam caller.

Caller reputation method is follows:

- Collecting CDR information
- Social network strength
- Direct trust
- Global reputation
- Automatic Threshold
- User involvement

CDR (CALL DETAILS RECORD)

A call detail records (CDR) are unavailable because of the privacy. We get the CDR data from crawdad website and we preprocessed it. CDR contains the data about data that is Meta data. It contains data fields that describe a specific instance of a telecommunication transaction, but it does not include the content of the transaction. CDR is a file that contains information about recent system usage like identities of sources, the identities of destinations, the duration of each call. For billing purpose they maintain the information of the amount billed for each call, the total usage time in the billing period, the running total charged during the billing period and the total free time remaining in the billing period. The way of simplistic example, CDR describing a particular phone call might include the phone numbers of the calling and receiving parties, the start of the call, and duration of that call. The call detail records contain attributes such as:

- the phone number receiving the call and the phone number of the subscriber originating the call
- the starting time of the call and call duration of the call
- the identification of the telephone exchange
- call type and any fault condition encountered

Table 1.Structure of CDR

Table 1.Structure of CDR

ID	Calling Party	Called Party	Date and Time	Call Duration	Call Type	Fault Condition
123	9710410829	9003095132	24-01-2012 12.05pm	5min	Voice	Success
114	9965320235	9443799049	24-01-2012 1.30pm	7min	Voice	Success
189	9965245068	8695976414	24-01-2012 1.30pm	10min	Voice	Success
117	9597994023	9940527033	26-01-2012 03.00pm	15min	Voice	Success
145	9965216667	9094862745	27-01-2012 10.15am	8min	Voice	Success
179	9971213141	9003095132	27-01-2012 01.30pm	3min	Voice	Success

The TRAI (Telecom Regulatory Authority of India) and CRM (Customer Relationship Management) contains the information about age of the Subscriber Identity Module (SIM) of user. The legitimate callers will not change the number frequently. But the spam callers have the behavior of changing the number frequently.

SOCIAL NETWORK FEATURES

A caller -callee social network graph is modeled in R Studio. R studio is advanced part of R tool. We can get the graph exactly in R studio. R Studio is an integrated development environment (IDE) for R. It includes a console, syntax-highlighting editor that supports direct code execution, as well as tools for debugging, plotting, history and workspace management [15]. Whenever the new user enter into the VoIP network the social network graph will be analyzed between caller S and callee R if S calls R at least once.

The number of phone calls received at an exchange or call center in an hour;

X has a Poisson Distribution with parameter λ and

$P(X = k) = f(k) = e^{-\lambda}.\lambda k / k!$, $k = 0,1,2,....$

The random variable X indicates the number of successes in the whole interval. λ indicates the mean number of successes in the interval.

The following parameters are usually used for analyzing the relationship between the caller and the callee:

- Indegree
- Outdegree
- Call rate
- Call duration
- Call intervals between the calls

In-degree represents the number of other different users calling this user and out-degree represents the number of calls made from this user to other unique users. The spam callers have the behavior of uni-direction of communication so, it is unbalanced in/out degree. But, the legitimate callers have bi-directional relationship so that it is balanced in/out degree.

Call rate is the total number of calls made/ received by the caller and it can be categorized as in and out call rates. Call rate says the repetitive behavior of user based on the higher call rate, more frequently user calls the same people. Spam caller have higher call rate only for outgoing, they don't have the repetitive behavior. Call duration is the total duration of the calls made or received by the user. The call intervals is the intervals between the consecutive calls.

The legitimate callers have higher amount of call duration with their social network and have small amount of duration with outside of their social network as shown in **Figure- 3**. Legitimate callers don't call the unknown numbers. But spam caller have the behavior of making calls to the unknown person. They make large number of calls with the small amount of call duration. The legitimate callers will call their social network repeatedly and they get reciprocal calls from their social network circle. So the number of unique outgoing calls i.e outdegree of the legitimate caller will be less.

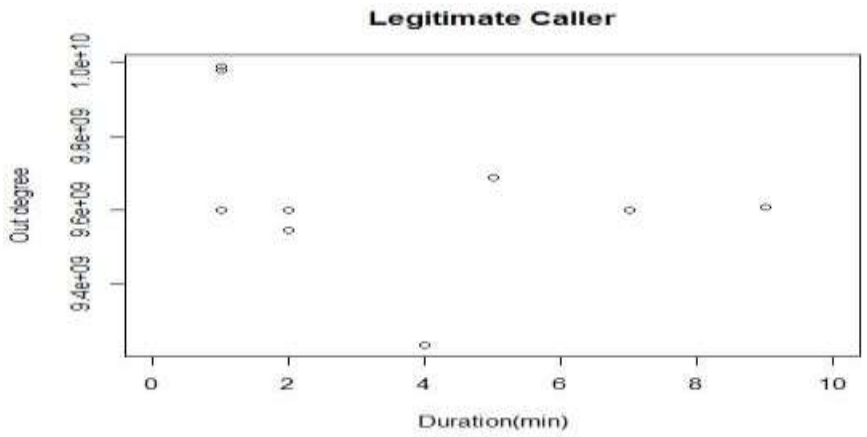

Fig: 3. Social network graph for legitimate user

The SPIT callers have lower amount of call duration with outside of their social network as shown in **Figure- 4**. Spam callers mostly call the unknown numbers. They make large number of calls with the small amount of call duration. The Spam callers will call unknown people repeatedly and they get very rare reciprocal calls. So the number of unique outgoing calls i.e outdegree of the spammer will be more.

THE IIOAB JOURNAL
ISSN: 0976-3104

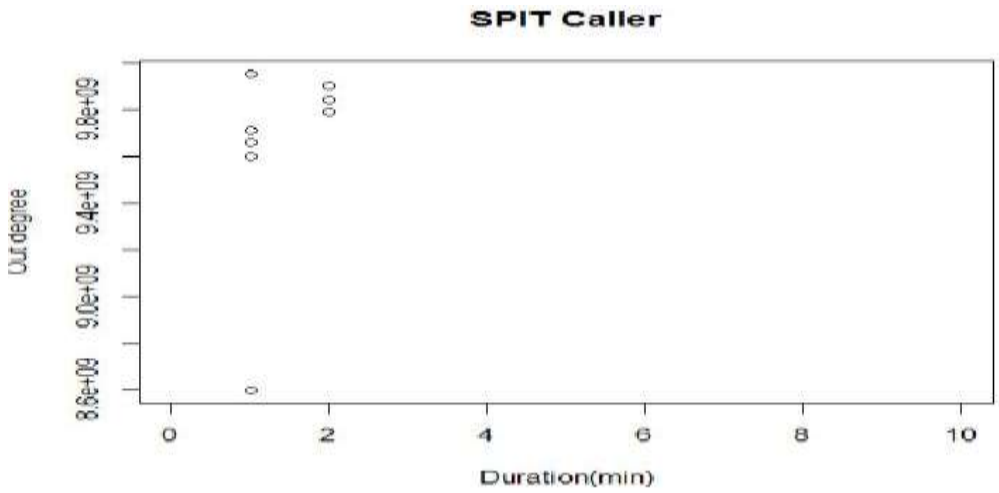

Fig: 4. Social Network Graph of a SPIT caller

THRESHOLD VALUE

The analysis shown in **Figure- 5** is a research done by San Francisco State University which includes A-B call pairs of a legitimate caller. The scanner locates the call information on a spectrogram by pixel coordinates and separates the call sequences by a longer breathing interval .The difference between the time of each call is calculated and plotted. The mean and the standard deviation of the recorded calls are calculated by using the iterative procedure which tries to fit the distribution to the Gaussian plus a uniform distribution. The calculated average time is 135.4 seconds with a standard deviation of 8.8 second. The distribution ranges between 100 and 150 seconds which is clear from the graph in **Figure- 3**.The threshold value is set as 100 seconds for the call interval method of finding the spammer in the IP telephony. The mean call interval of the caller is checked by the SIP server before setting the call connection. The caller with lesser mean call interval is considered as spammer and such calls are blocked before setting up the call i.e the pre acceptance method.

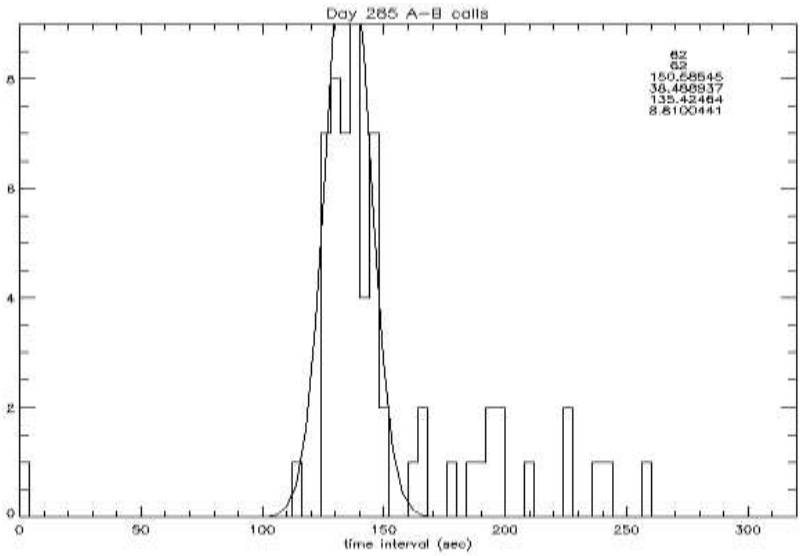

Fig: 5. Distribution of time intervals for Legitimate caller monitored for 285 days

TYPES OF SMS MESSAGE

There are four classes of SMS message . These Classes identify the importance of an SMS message and also the location where it must be stored.

- **Class 0**
  This type of SMS message is displayed on the mobile screen without being saved in the message store or on the SIM card; unless explicitly saved by the mobile user.
- **Class 1**
  This message is to be stored in the device memory or the SIM card (depending on memory availability).
- **Class 2**
  This message class carries SIM card data. The SIM card data must be successfully transferred prior to sending acknowledgment to the service center. An error message is sent to the service center if this transmission is not possible.
- **Class 3**

This message is forwarded from the receiving entity to an external device. The delivery acknowledgment is sent to the service center regardless of whether or not the message was forwarded to the external device.

The OTP (one time password) will be any one of the class based on the developer. A **one-time password** (**OTP**) is a password that is valid for only one login session or transaction, on a computer system or other digital device. A spam caller who makes bulk calls trough IP telephony for advertisement or in call center will never use that number for authentication purpose. So IP Telephony numbers that receives OTP sms is taken as one of the parameter for segregating the legitimate caller.

SPIT DETECTION ALGORITHM

Algorithm . SPIT Detection

1. *Start the call detail log record*
2. *Assign call detail vector X for each caller*
3. *Define Matrix M with call interval element*
4. *Calculate* $\mu = \sum M$ *of X*
5. *Compare with the threshold value* β
6. *If* $\mu < \beta$ *then calculate the online reputation score*
7. *{ If online reputation score is equal to NULL then report as spam caller*
8. *Else report as legitimate caller }*
9. *Else report as legitimate caller*
10. *Stop*

SIMULATION RESULTS

The spit detection algorithm is stimulated in the WiMax environment . The Wimax wireless technology that uses the VOIP for transmitting the voice with the existing hardware and software.When spamming nature is introduced to one of the node in the network the performance of the network is found to degrade. The spammer is detected using the above algorithm and the saved bandwidth is calculated.

This scenario for the bandwidth calculation is a wireless network with four base stations and twenty subscriber stations (fixed node) is shown in fig 6.The topology consist of geographical overlay of four cells ,each with radius 3km and 20 subscriber stations. The nodes are placed in a random manner. Out of the 20, one of the node circled in red is simulated to generate unwanted spam calls. Main considerations made in our simulation while deploying wireless network are technology and topology.

Technology : WiMAX technology with subscriber node transmission power 0.5 w and base station transmission power 0.5w.

Topology : The simulated topology consist of 4 hexagonal cells with cell radius of 3km.Number of subscriber stations per cell is 20.Base stations are modeled with wimax_3section_bs_atm2_ethernet2_slip4_wlan_router. The subscriber stations are modeled with wimax_ss_wkstn.

Fig: 6 . WiMax Scenario taken for simulation

This topology is designed for VOIP application that is both voice application. The configurations used in the above simulated scenario are profile config, application config and wimax config.

Application Config : This specifies the various application used in the project. The various application names are web browsing, FTP, databases, HTTP, remote login, voice and video conferencing. In the above simulation we have taken the voice and video conferencing.

Profile Config: It is used to create the traffic pattern for the application defined in the application config.

Wimax config : It is used to store profiles of physical and service classes which can be referenced by all wimax nodes in the network.

Table 2.Simulation Parameter

Parameter	Value
Network interface type	Phy/Wireless Phy/OFDMA
Propagation model type	Propagation/ OFDMA
Medium Access Control type	Mac/802_16/Base Station
Routing protocol	VOIP
Antenna model	Antenna/Omni Antenna
Link layer type	Logical Link layer
Frame size (msec)	5 (msec)
Duplex scheme	TDD
Packet Rate	4 packet/s

Bandwidth Utilized by the spammer

1 Hour	7200KB
3 hours	21600KB
9 hours	64800KB

1 day(app 12 hours)	86 MB

CONCLUSION

The call interval method of spam detection is computed using Algorithm 1. Our system is used to analyze the call detail record to find whether the user is spam caller or legitimate caller. The CDR contains the private information of who, when and duration of every call. The CDR also has the information of all the sms delivered and sent of each user. The blocking of the spam caller before setting the call will save the bandwidth and avoid congestion of the network.

CONFLICT OF INTEREST

The authors declare no conflict of interests.

ACKNOWLEDGEMENT

None

FINANCIAL DISCLOSURE

None.

REFERENCES

[1] Ricardo Morla, Muhammad Ajmal Azad. [2013] "Caller-REP: Detecting unwanted calls with caller social strength, ELSEVIAR, Pages 219–236.

[2] Gamal A. Ebrahim. [2013] A VoIP SPAM Reduction Framework, *IEEE*.

[3] Dirk Lentzen, Gary Grutzek, Heiko Knospe, Christoph Porschmann. [2011] Content-based Detection and Prevention of Spam over IP Telephony - System Design, Prototype and First Results, *IEEE*

[4] Kentaroh Toyoda, Iwao Sasase. [2013] SPIT Callers Detection with Unsupervised Random Forests Classifier, *IEEE*

[5] Yan Bail, Xiao Su, Bharat Bhargava.[2009] Detection and Filtering Spam over Internet Telephony - A User-behavior-aware Intermediate-network-based Approach, IEEE

[6] He Guang-Yu, Wen Ying-You, and Zhao Hong. [2008] SPIT Detection and Prevention Method in VoIP Environment , *IEEE*

[7] Dongwook Shin. [2006] Progressive Multi Gray-Levelling: A Voice Spam Protection Algorithm, *IEEE*

[8] Mohammad Hossein Yaghmaee Moghaddam, Mina Amanian, Farideh Barghi, and Hossein Khosravi Roshkhari.[2014] A Survey of Different SPIT Mitigation Methods and a Presentation of a Comprehensive SPIT Detection Framework, *International Journal of Machine Learning and Computing*, 4(2)

[9] Christoph Sorge, Jan Seedorf. [2009] A Provider-Level Reputation System for Assessing the Quality of SPIT Mitigation Algorithms, *IEEE* ICC

[10] Tetsuya Kusumoto, Eric Y. Chen, Mitsutaka Itoh. [2009] Using Call Patterns to Detect Unwanted Communication Callers, *IEEE*

[11] Vijay A. Balasubramaniyan, Mustaque Ahamad, Haesun Park. [2007] Call Rank: Combating SPIT Using Call Duration, Social Networks and Global Reputation", CEAS, Fourth Conference on Email and Anti Spam, August 23, 2007

[12] Fei Wang, Yijun Mo, Benxiong Huang. [2007] P2P-AVS: P2P Based Cooperative VoIP Spam Filtering, *IEEE*

[13] https://books.google.co.in/books?id=WN4JANNzkJoC&p

[14] http://icsa.cs.up.ac.za/issa/2005/Proceedings/Research/09 1_Article.pdf

[15] http://www.rstudio.com/products/rstudio