A Joint Port and Statistical Analysis Based Technique to Detect Encrypted VoIP Traffic

Suneel Munir[1*], Nadeem Majeed[2], Salaser Babu[3] , Irfan Bari[4], Jackson Harry[5], Zahid Ali Masood[6#]

[1,2,3,4,5] University of Engineering & Technology, Taxila
[6]COMSATS Institute of Information Technology, Islamabad

Abstract

VoIP is rapidly growing technology due to its cost effectiveness, dramatic functionality over the traditional telephone networks and its compatibility with public switched telephone network (PSTN). Detection of VoIP is important for telecommunication authorities, internet service providers, and governmental law enforcement agencies for blocking, prioritizing, monitoring and electronic surveillance. Modern VoIP applications use dynamic ports, proprietary protocols, encryption, obfuscation and anti reverse-engineering procedures leaving port-based techniques, signature-based techniques and pattern-based detection ineffective. For generic purpose, only statistical techniques can be used for better results but existing statistical analysis-based detection techniques have some limitations and cannot provide more efficient and accurate solutions. In this paper, we proposed a hybrid solution based on port number and statistical analysis using threshold values of flow statistical parameters to detect the VoIP media (voice) flows.The solution is generic, efficient, accurate, real time (to some extent) and can detect encrypted, plain and tunneled VoIP traffic. The proposed system is evaluated for accuracy, efficiency, and scalability. It has 97.165% detection rate (DR) and 2.68% false positive rate (FPR). It can detect VoIP calls from any VoIP application or protocol within 6 seconds. The proposed system shows better results and hence can fulfill the need of telecom operators and ISPs for detecting VoIP.

Keywords: VoIP, Encryption, Statistical analysis, Flow, Detection Rate (DR), False Positive Rate (FPR)

1. Introduction

Voice over Internet Protocol (VoIP) usage is increasing day by day due to its low cost and dramatic functionalities. The adoption of VoIP is not without its complications. The commercial usage of VoIP is prohibited in many countries, as it incurs loss in profit to their telecommunication industries. Internet service providers also desire to prioritize VoIP for their paid customers. Government and law enforcement agencies are also concerned in tracking down VoIP traffic in real time to counter any vicious activity. Not only this, many VoIP applications are prone to number of P2P vulnerabilities such as buffer overflow and denial of service attacks. VoIP applications also make direct connections with unknown clients so they can be exploited by viruses, worms and Trojan. All these problems affect the productivity and efficiency of large organizations. So detection of VoIP has become a hot area of research. Use of complex encryption and tunneling mechanisms for VoIP makes detection very difficult. VoIP signaling and media transmission both may be encrypted or any one may only be encrypted. Different techniques exist to detect VoIP traffic. These techniques are divided into 6 basic classes i.e. port-based, signature-based, pattern-based, statistical analysis-based, machine learning based, and hybrid detection techniques. Each type of technique has some limitations. Some of these techniques are rarely used nowadays, due to complex, confidential and secure privacy protocols. Also with the development of new VoIP applications and technologies, the detection of VoIP is becoming

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

more and more difficult. So it is very hard to come up with a solution that can detect VoIP with 100% of accuracy and efficiency.

In this paper we proposed a hybrid solution based on port number and statistical analysis using threshold values of flow statistical parameters to detect the VoIP media (voice) flows. The solution is generic, efficient, accurate, real time (to some extent) and can detect encrypted, plain and tunneled VoIP traffic. The remainder of this paper is organized as follows. InSection 2 we briefly describe related work. In Section 3 we introduce our classification methodology, showing how we carried out statistical analysis and what observations we took to built our own proposed system. Section 4 is about proposed system, which describes threshold rules and algorithms to detect VoIP and non-VoIP traffic. In Section 5 we evaluated our system for accuracy, efficiency and scalability. Finally Section 6 concludes the paper.

2. Related work

The main steps that are involved in VoIP call setup are signaling and media channel setup (voice transmission). The detection techniques can be applied on any of these two steps. Some techniques detect VoIP traffic by examining signaling traffic and others detect VoIP by examining media traffic. Some techniques exists that examines both signaling and media traffic. In this section we provide basics of VoIP and moreover we review existing VoIP detection techniques and approaches and the recent work that has been done using these techniques. There are basically 6 types of techniques that are used to detect VoIP traffic flows.

2.1 Port based detection techniques

The simplest, robust and fastest of the detection technique is port based detection. This approach allows fast flow classification because port number can be easily accessed and are generally not affected by encryption. Table 1 shows some of standard ports for specific VoIP applications by IANA.

Sr. No.	VoIP Protocol	Port Number	Default Transport Layer Protocol
1	SIP	5060-5070	TCP/UDP
2	H.323	1718-1720	TCP/UDP
3	MGCP/Megaco /H.248	2427,2944	TCP/UDP
4	Skype(client login)	80,443	TCP
5	Skype (authentication)	33033	TCP

Table 1: VoIP protocol and standard ports specified by IANA

By port-based analysis if these ports are used at transport layer, the flow is detected as VoIP. Leung et al, in [1] used port numbers as helping information to detect VoIP. Renal at el, in [2], detected Skype VoIP traffic by matching distinct Skype keywords, ports, and content. Port based detection techniques are easy to implement and fast but less accurate as non standard ports are used by modern VoIP applications. Moreover the ports are dynamically allocated and in case of IP layer tunnels, the transport layer information is hidden. So in these cases this technique is useless and produces incorrect results

2.2 Signature based detection techniques

Signature-based techniques are also called as protocol decoding techniques. A signature-based detection method classifies the internet traffic by matching specific strings within packet payload for that protocol [3]. It detects VoIP using deep packet inspection. Each VoIP protocol has distinct signatures that can be used for detecting VoIP traffic. Signature-based detection techniques in [2, 4-6] detect VoIP flows by VoIP application signatures. Renal et al, in [2] proposed a signature based approach to block Skype traffic. They discovered that the Skype packets contain the keyword “/getlatestversion?ver=" or /getnewestversion" combined with a “/ui/" string. Table 2 shows some distinct signatures of various VoIP protocol and applications. The signature-based detection techniques are easy to implement, fast and efficient for un-encrypted data but these are ineffective for encrypted and tunneled data as it modifies the signatures.

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

Sr. No.	VoIP Protocol	Signature	Place to Find
1	SIP	"sip"	Application data
2	RTP/ SRTP	0x80,0x81	RTP header, after transport layer Header
3	ZRTP	"1000xxxx5a5 25450	header, Payload
4	Skype login	"16 03 01 00 ** 42 cd ef e7 40 d7"	Payload, within transport layer Packet
5	Skype (contents)	"/getlatestversion?ver="	Payload, within transport layer packet

Table 2: VoIP protocols and applications signatures

2.3 Pattern based detection techniques

Pattern based detection techniques are proposed to handle the shortcomings of port and signature based detection techniques. In Pattern-based detection techniques the particular pattern of signals between communication parties is identified. These techniques are powerful for the detecting those VoIP applications that use proprietary protocols for signaling i.e. Skype. Pattern based detection techniques are proposed in [1, 4, 6, 7]. In [1] pattern based detection along with port based detection is proposed to detect Skype Traffic. The researcher used forensic approach to investigate the Skype by deeply investigating the Skype communication. They also discussed 15 basic stages of Skype communication from start to end. Feng et al, in [4] used a joint port-based and pattern-based techniques to detect VoIP traffic. They analyze the Skype protocol with respect to its general and behavioral characteristics and used them to identify the Skype traffic to block it. Uzma et al. [7] in 2014 proposed a pattern based approach to detect illegal VoIP traffic using Call Detail Records. They used sip signature "sip" in the Skype signaling traffic to identify VoIP traffic. Pattern based detection techniques works well in some cases to detect encrypted VoIP but they are dependent on specific VoIP application. The signaling mechanism may vary from application to application, making it less accurate and inefficient.

2.4 Statistical analysis based detection techniques

Traffic classification techniques which need to access the payload of the packets do not work always for the identification of all protocols. Indeed, in order to protect the user's privacy, some legal restrictions are imposed to prevent the access to the payload of the packets. Not only this, if the payload of the packet is encrypted, the access to the payload is also prevented. To overcome all these limitations, the statistical analysis based detection approaches came into research [3, 8-17]. By statistical techniques, some statistical measures are taken on flow features such as mean, standard deviation (S.D) of packet sizes and the packet arrival time measures are used for VoIP detection. Statistical analysis is mostly performed on voice data but it can also be performed on signaling data. Yildirim et al.[10] in 2010 proposed a simple VoIP traffic classification method. The authors used the packet length as the statistical measure to mark a packet. They proposed that the packet will be a VoIP packet if its size is between 60 and 150 bytes. Piskac et al. in [16] proposed a statistical method to classify traffic using the time characteristics of the data flow. Statistical measures like number of packets and their size in bytes, S.D, Mean, minimum difference, maximum difference of the inter-arrival time of packets in a flow are used to classify VoIP traffic. On bases of these values the vector for each packet and each flow is formed. The authors also used Euclidean distance, Root-Mean-Square distance and the angles between the vectors to calculate the associations between the different vectors. The proposed approach has TPR of about 90% and FPR of 7% respectively. Fauzia et al, in [11] proposed a generic technique to detect the VoIP traffic generated by different VoIP protocols. They perform some statistical analysis on the traffic and separate out the VoIP media traffic by using traffic features that are difficult to alter such as packet interval time, packet sizes, rate of exchange. Freire et al, in [12] proposed a solution that detects the VoIP calls hidden in web traffic such as Gtalk and Skype traffic. The authors analyzed the media traffic by taking parameters such as web request size, web response size, inter arrival time between requests, no. of requests per page, page retrieval time. They use goodness of fitness test, the Kolmogorov-Smirnov (KS) distance and chi-square values and obtain metrics to identify the VoIP in web traffic. The scheme considers the key

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

characteristics of normal behavior of web traffic (HTTP, HTTPS) and matched it to the actual traffic to identify VoIP. Yildirim et al. proposed statistical technique [10] to identify VoIP protocol within encrypted tunnel. They use probabilistic information of traffic to identify application protocols in tunnels. Their decision algorithm does Packet size distribution on packets that lies with a specified size range. Ying-Dar et al. [8] also proposed a generic technique to classify the network traffic into different application types. They use packet size distribution (PSD) and assume that each application has a distinct PSD. They also use the port association techniques while classifying traffic by which if a port is consecutive to the previously identified flow port then it is detected as the part of the previous flow. Toshiya et al, [15] in 2006 proposed Flow level behavior (FLB) VoIP detection technique. They also used packet size and inter-arrival time to classify VoIP traffic.

2.5 Machine learning based detection techniques

In addition to normal statistical analysis for data classification, many researchers are now interested in heuristics and statistical-based traffic classification using machine learning algorithms. Machine learning algorithms can create a data model from a given dataset automatically. The created data model comprises of a decision tree or a decision table which selects the best suitable attributes and threshold values for data classification. Machine learning based detection techniques are discussed in [18-26]. Riyad et al. [26] used ML to detects the VoIP traffic by using flow features, such as size and time. They evaluated the three different machine learning (ML) algorithms C4.5, AdaBoost and Genetic Programming (GP) under data sets common and independent from the training condition. Two VoIP applications Skype and Gtalk are tested. Their result shows that C4.5 has the best performance with DR 99% and FPR less than 1%. Riyad et al. [21, 25] extended their previous research work to detect encrypted VoIP traffic by using machine learning techniques. They applied three ML algorithms to test more data traces produced by different application. They deployed three supervised learning algorithms, namely C5.0, AdaBoost and Genetic Programming (GP), to generate signatures automatically to robustly classify VoIP encrypted traffic. Their results show that C5.0 performs much better than GP and AdaBoost algorithms in detecting encrypted VoIP traffic. They demonstrate that C5.0 algorithm can also accurately differentiation between multiple VoIP applications without employing port numbers, IP addresses and payload information. Lam H et al, [27] in 2009 proposed a machine learning based traffic detection system to classify Skype, VoIP and other traffic. They used packet length and inter-arrival time between packets as statistical features to identify VoIP flows. Despite calculating statistical parameters on complete flow they used short sliding window of 10 seconds. The proposed solution is almost real time, producing accuracy of 99%. Zander et al, [18] in 2005 proposed ML based traffic classification and application identification technique by using an unsupervised machine learning. The researcher used (SFS) Sequential Forwarding Selection to find the best attributes from the dataset. The statistical attributes considered were packet inter-arrival time, packet length mean, packet length variance and flow size in bytes. To evaluate the quality of results a metric called as intra-class homogeneity H. Higher homogeneity H was required for better traffic classification. The average accuracy of their proposed technique was 86.7%. Support Vector Machine (SVM) is considered as one of the best machine learning algorithm for classification purpose. SVM has some distinctive features, such as small sample sets, high accuracy, ability for simultaneously minimizing the empirical classification error and maximizing the geometric margin classification space and strong generalization performance. Beside network traffic classification it can be applied to text categorization, image recognition and motion classification. SVM based ML techniques in [23, 24] are used for traffic classification. S. Anu et al. [24] in 2014 proposed Support Vector Machine (SVM) based network traffic classification technique. The researchers compared the classification performance of SVM with Naive Bayes, C4.5 and K-NN method. Their result shows that SVM has better classification accuracy than other three models. Statistical approaches are good and produce better results in case of encrypted VoIP. The results of statistical approaches are better than other approaches on latest VoIP applications but still the existing statistical techniques are not so efficient for IP layer tunneled VoIP detection. Moreover most of the statistical approaches are not

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

real time and need prior captured traffic to analyze. So these systems could not be practically implemented to block or prioritize VoIP efficiently and accurately with best results.

2.6 Hybrid detection techniques

To gain the advantages of multiple approaches and overcoming the limitations of above mentioned techniques, the hybrid VoIP detection techniques are proposed. The hybrid techniques produce better results than individual technique. Hybrid detection techniques are discussed in [1, 6, 28] [18, 19, 24, 25]. Pattern-based analysis with port-based analysis are used in [18, 19] for Skype traffic detection. D. Adami et al, in [29] proposed a pattern and a port-analysis based hybrid technique to detect Skype traffic. The author analyzed Skype for Skype UDP ping, Skype UDP probe, Skype TCP handshake, and Skype authentication both statistically and behaviorally.

D. Adami et al, in [28] proposed a hybrid technique for detecting Skype traffic. Both signature-based and statistical approaches are used in parallel producing best results. The proposed system outperforms the classical statistical analysis based detection classifiers as well as the state-of-the-art ad hoc Skype classifier. Robert B. et al, in [30, 31] presented an extensive measurement campaign focusing on VoIP traffic characterization. The researcher proposed a heuristic algorithm based on joint signature, port and statistical analysis based hybrid techniques to identify RTP/RTCP traffic.

The comparison of discussed techniques is shown in Table 3

Detection Technique	Applied on	Scalability	Performance Speed	Encryption support
Port based	Signaling, voice	Application and Protocol Specific	Good	Yes, other than IP tunneling
Signature based	Signaling, voice	Application and Protocol Specific	Better	No
Pattern based	Signaling	Application and Protocol Specific	Better	Limited
Statistical analysis based	Mostly on voice	Generic	Bad	Yes
Machine Learning	Mostly on Voice	Generic	Bad	Yes
Hybrid	Signaling, Voice	Generic	Bad	Yes

Table 3: Comparison of VoIP Detection Techniques

Each of the discussed technique has some limitations. Statistical, machine learning and hybrid detection techniques normally works well in generic. So there is a need of an accurate, generic, efficient, real time and practically implementable statistical analysis-based or hybrid solution that can detect encrypted, non-encrypted and tunneled VoIP. The detection algorithm should not be dependent on any VoIP application, protocol, security mechanism, or any tunneling mechanism.

3. Methodology

We considered the most famous VoIP applications of modern days, and analyzed the traffic traces produces by them. The data for traffic analysis is obtained from NARC of University of engineering and technology Taxila, home users, sample traces from Wireshark and tstat sites.

For experimental analysis we considered the traffic traces of common VoIP applications like facebook messenger, viber, skype, google hangouts and

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

yahoo messenger as testing applications. In addition to these applications, traffic traces of various non-VoIP applications and services are also analyzed such as online gaming, torrents (bittorent, utorrent),antivirus updates (MS Security Essentials, Kaspersky), online streaming/online tv, audio video streaming, download Manager, FTP, chat applications (Yahoo, Gmail, MSN), web browsing and Emailing. We used wireshark and weka as analysis tool.

3.1 Statistical analysis

The main statistical parameters we are used to analyze each flow are, packet-rate, mean and standard deviation of packet sizes, maximum difference time, mean and standard deviation of maximum difference time, entropy and data rate. : No. of packets in seconds. Packet rate of the flow in packets/sec

- Mean(Avg. size) : Mean (average) of IP layer (layer 3) packets sizes of the flow in bytes
- S.D (size): Standard deviation of IP layer (layer 3) packets sizes of the flow in bytes
- Max-diff-time: Maximum difference between the current and previous packets' time for all packets of the flow in seconds
- Mean(diff-time): Mean (average) of the difference between the current and previous packets times in seconds
- S.D (diff-time): Standard deviation of the difference between the current and previous packets times of the flow in seconds
- Data rate: No. of Mbs in seconds.
- Entropy (H): Measure of the degree of uncertainty of a given random variable

The statistical analysis is performed on traces by two ways; firstly, the statistical parameters are calculated and analyzed for each flow of complete session without considering time limit. In real circumstances, it makes no sense to identify Internet flows when they have ended. The early identification of the flow is very essential to apply the subsequent management and security policies. In the second phase we analyzed statistical parameters of each flow by adopted sliding window of 5 seconds, means data for first 5 seconds of the each flow is captured and analyzed. Table 4 and 5 shows statistics of VoIP and non-VoIP traffic traces.

Statistical Parameters	**Google + hangouts**	**Facebook VoIP**	**Yahoo messenger**	**Skype 7.2.2**	**Viber**
Time	3m21s	2m46s	2m6s	5min	1m42s
Packets	15200	4101	5200	30367	7322
Packet rate(p/sec)	68	24.7	41.27	101	71
Mean (P_Size)	73.5	107	92	135	130
S.D (P_Size)	38.88	41.115	18	28	41.26
Max_diff_time	0.19	0,.232	0.099	0.138	0.39
Mean(diff_time)	0.055	0.069	0.0299	0.028	0.0477
S.D(diff_time)	0.041	0.045	0.022	0.026	0.048
Data Rate (Mb/sec)	0.481	0.028	0.031	0.119	0.074
Entropy (H)	3.29	2.78	3.17	3.77	8.24

Table 4: Statistical results of VoIP traffic traces

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

Statistical Parameters	Online TV	torrent	Yahoo text chat	Game play	Youtube	Antivirus update	Download Manager/FTP	Web Browsing
Time	3m2s	3m40s	3m52s	9m5s	1m39	1m20s	5mins	2m52s
Packets	39476	145984	208	1145	8671	529	148434	4646
Packet rate (p/sec)	78	663	0.89	31	87	6.612	495	27
Mean(P_size)	746	845	168	581	876	386	1034	506
S.D(P_size)	106	117	40	653	683	593.18	663.5	598
Max_diff_time	0.331	0.475	0	0.341	0.177	0.254	0.426	0.343
Mean(diff_time)	0.023	0.047	0	0.024	0.009	0.023	0.047	0.0295
S.D(diff_time)	0.0588	0.097	0	0.061	0.232	0.058	0.094	0.0738
Date Rate (Mb/s)	0.331	3.978	0.001	0.0031	0.616	0.051	4.088	0.109
Entropy (H)	0.882	1.866	2.01	1.287	0.773	0.014	1.445	1.357

Table 5: Statistical results of non-VoIP traffic traces

3.2 Key observations from statistical analysis

From the statistical analysis we noticed following findings

a. The average packet size and standard deviation of VoIP data is much smaller than non-VoIP.

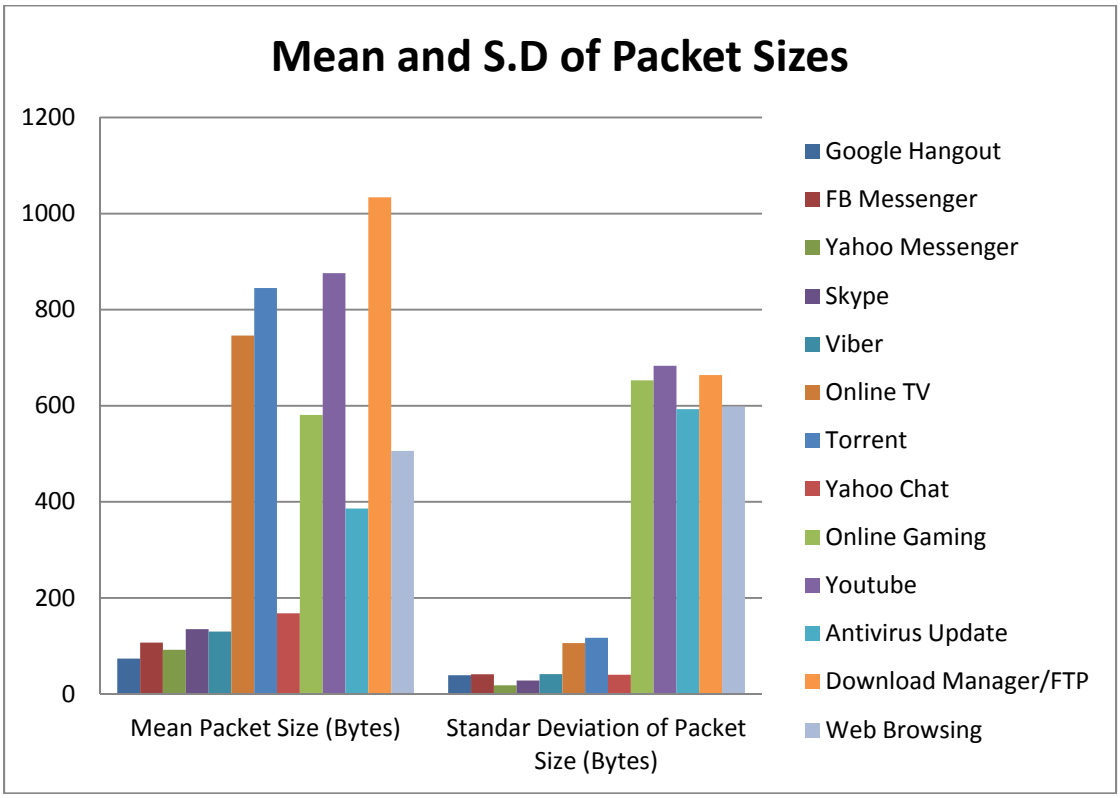

Figure 1: Mean and S.D of VoIP and non-VoIP traffic traces

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

b. The packet rate of VoIP is greater than some non-VoIP applications

The packet rate of non-VoIP chat applications, web browsing and antivirus update is lower than VoIP. On the other hand torrent and download managers have higher packet rates.

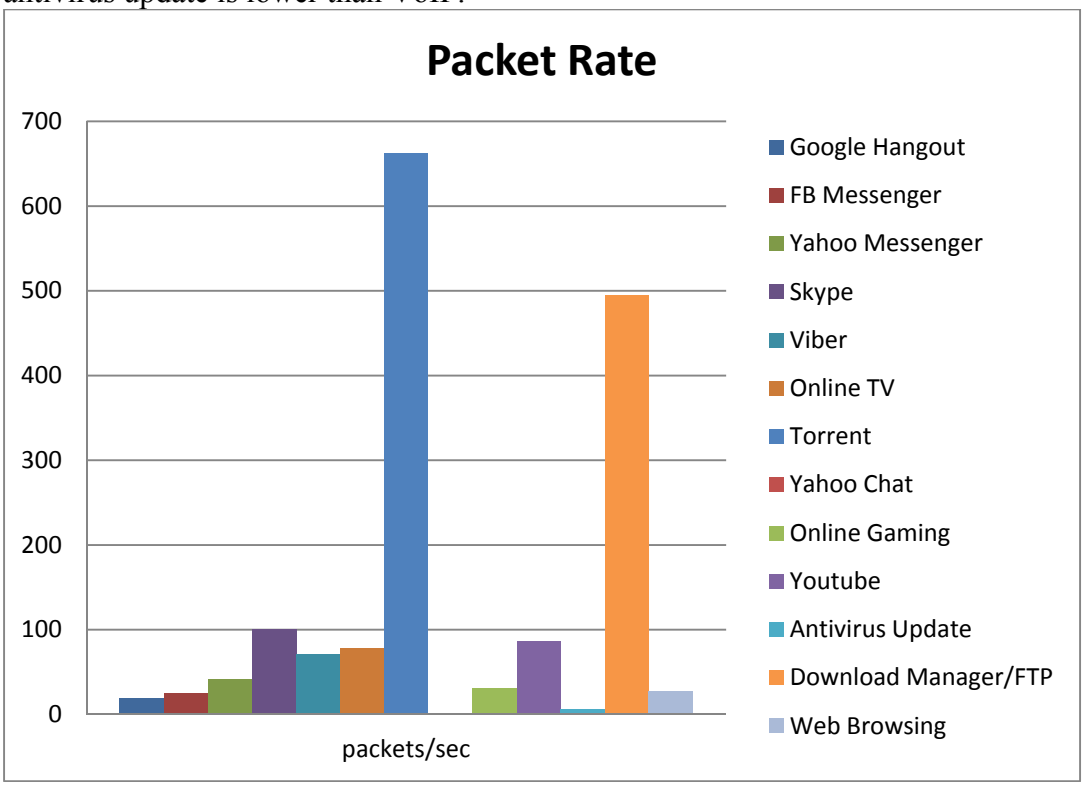

Figure 2: Packet rate of VoIP and non-VoIP traffic traces

c. The entropy (H) of VoIP is greater than non-VoIP traffic traces

Entropy has been used in different fields of study and therefore has several interpretations. It is defined as measure of the degree of uncertainty of a given random variable. Entropy is denoted by H(n) where n represents number of values in the observation pool, and p(xi) denotes the probability of occurrence of a given value xi. Entropy is represented by the expression (1).

$$H(X)= -\sum_{i=0}^{n} p(xi)\ln\left(p(xi)\right) \qquad (1)$$

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

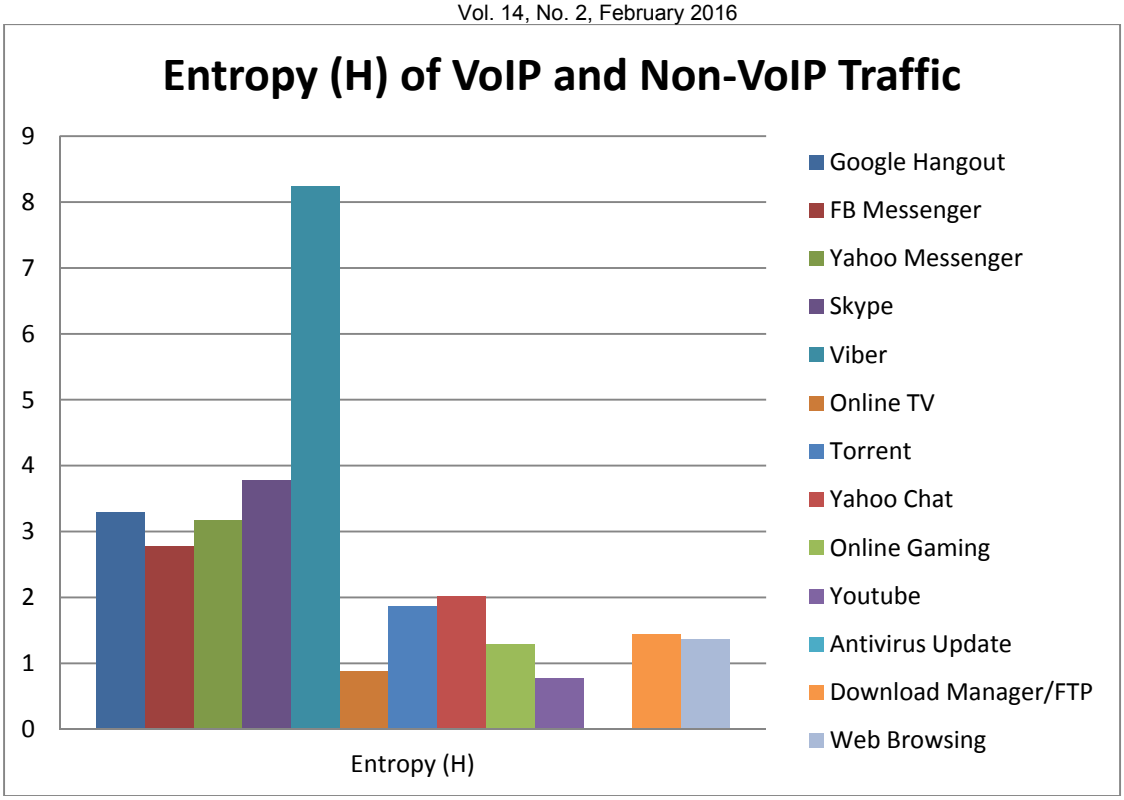

Figure 3: Entropy of VoIP and non-VoIP traffic traces

d. The data rate of VoIP is smaller than some of non-VoIP data.

Torrents and download managers have higher data rate than VoIP.

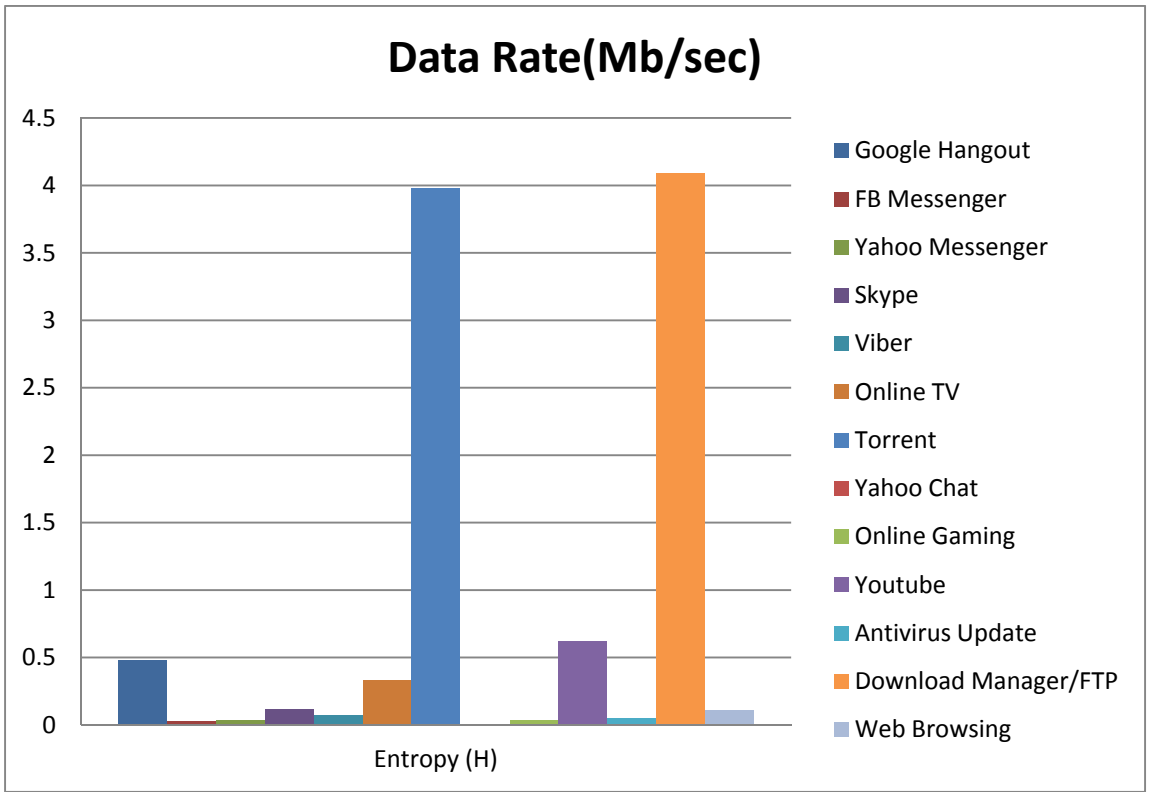

Figure 4: Data rate of VoIP and non-VoIP

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

4. Proposed System

On the bases of experimental analysis we proposed a system which can identity VoIP efficiently and accurately.

4.1 Flow registration process

Firstly each flow is registered. The proposed system distinguishes each flow by 4 tuples (Source-IP, Destination-IP, Source Port, and Destination Port). It is useless to identify the flow after it has been ended. Therefore we focus our research on early identification. For this purposes the traffic of first 5 seconds for each flow is captured to calculate the statistics. After flow is registered, set of rules are applied to it to identify the flow as VoIP or non-VoIP. We set these nine rules for VoIP traffic detection.

1. Packet Rate > 15 packets/sec
2. Data Rate < 0.5 Mb/s
3. 50 ≤ Mean(packet size) ≤ 210 bytes
4. 0 ≤ S.D(packet size) ≤ 75 bytes
5. Mean(packet size) ≥ S.D (packet size)
6. Mean H(Packet Size) ≥ 3.0

All 6 rules must be true

7. 0 < max-diff-time ≤ 0.8 seconds
8. 0 < Mean (diff-time) ≤ .09 seconds
9. 0 < S.D (diff-time) ≤ 0.25 seconds

At least 2 rules from 3 must be satisfied

Figure 5 shows the flow diagram of VoIP detection process. If first 6 rules are true and none of the last three rules are satisfied than the flow is re-registered again. The traffic of next five seconds of the particular flow is captured again and statistics are calculated. If none of the last three rules are satisfied for three times, then the flow is marked as non-VoIP.

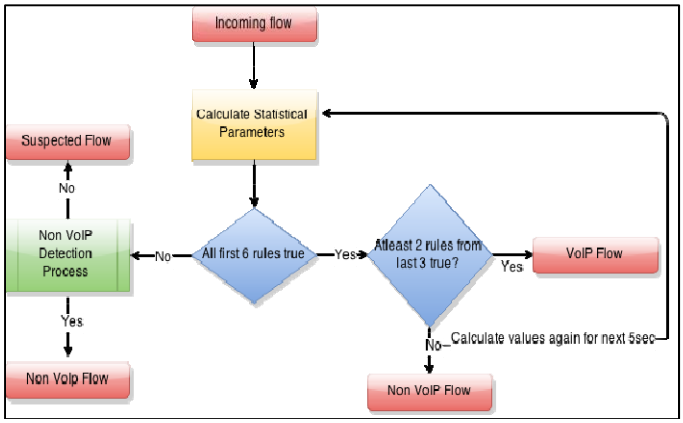

Figure 5: VoIP detection Process

4.2 VoIP detection process

A flow will be VoIP if all first 6 rules are true and if it satisfies 2 from last 3 rules.

4.3 Non-VoIP detection process

If any of first 6 rules is false then non-VoIP process is called to verify it as non-VoIP or suspected flow. From statistical analyses we have noticed that some of non-VoIP applications do satisfies rule 1 and 2. If first two rules are true and none of the rules from 3, 4, 5, and 6 are satisfied then the flow is termed as non-VoIP flow otherwise it is termed as suspected flow. A suspected flow is one that cannot be identified as VoIP or non-VoIP. It means that the system is unable to decide and evaluate the flow. Figure 6 show the flow diagram of non-VoIP detection process.

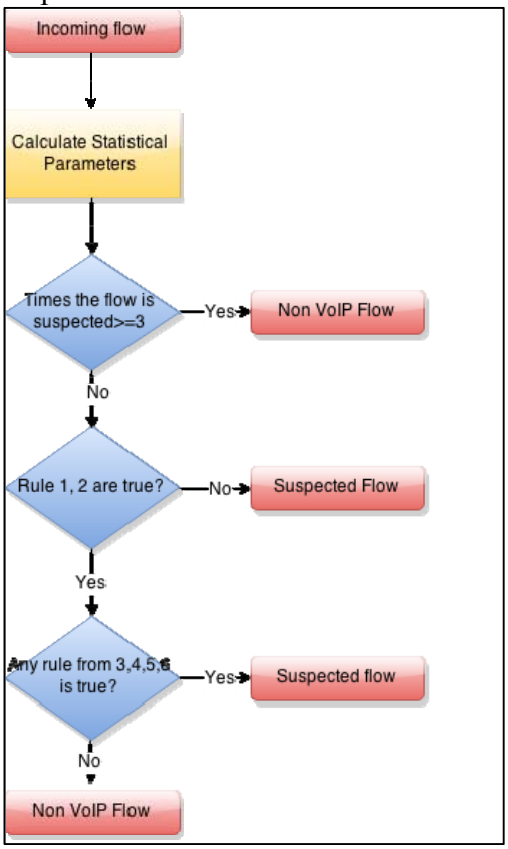

Figure 6: Non-VoIP detection process

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

4.4 Proposed system for detecting VoIP in IPSec tunnels

Internet Protocol Security (IPsec) is a protocol suite that secure the Internet Protocol (IP) communication by encrypting and authenticating each IP packet of a communication session [32]. IPSec operates in two modes, transport mode and tunnel mode. Payload data is encrypted in transport. When IPSec operates in tunnel mode, the whole IP packet is encrypted, authenticated or both, which means that IP packet is encapsulated into a new IP packet with a new IP header. The new IP header hides the transport layer information and hence we will have no knowledge of transport layer ports. The only available information is IP layer information so to detect VoIP in IPSec tunnel the proposed system needs little variation. Instead of distinguishing flows by 4 tuples (S-IP, SP, D-IP, DP) we will distinguish flows by 3 tuples (S-IP, D-IP, SPI). Security Parameter Index (SPI) is an essential part of IPSec which serves as an identification tag added to the header. SPI works like works like port numbers in TCP and UDP connections. For each flow we calculate statistical parameters and implement all nine rule mentioned in section 4.1. The same detection algorithm is used for detection of VoIP flows hidden in IP Layer tunnels with slight variations. The main points that are different from previous algorithm are as follows:

i. Each flow will be distinguished by 3 tuple (S-IP, D-IP, SPI)
ii. Remove the size of IPSec headers from overall IP Layer packet size while calculating statistical parameters related to size.
iii. Rest of algorithm will be same.

5 Performance evaluation of proposed system

To evaluate our proposed system w.r.t accuracy, efficiency and scalability, we implemented it in C++ using winpcap library. We collected different datasets and captured network traces from different locations such as tstat[33] and wireshark[34] sites. We also captured our own VoIP and non-VoIP traffic traces for evaluation. Table 6 and 7 shows the traffic traces for evaluating performance of the proposed system.

Trace	**Codec**	**Transport Layer protocol**	**Size (MB)**	**Duration (Sec)**
E2E-140606-1	G729	UDP	8	905
E2E-140606-1	iLBC	UDP	11	1003
E2E-140606-3	iSAC	UDP	12	1116
SkypeOut-260906-1	G729	TCP	9	919
SkypeOut-260906-1	G729	UDP	8	910
Internet-E2X-29		TCP	207	343546
Internet-E2E		UDP	4GB	344700
Internet-E2O		UDP	264	343562

Table 6: Downloaded traffic traces from tstat site for performance evaluation

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

VoIP			**Non-VoIP**		
VoIP traffic traces	**Size (MB)**	**Duration (seconds)**	Non-VoIP traffic traces	**Size (MB)**	**Duration**
Google hangouts	12	3m21s	Online TV	36.8	3m2s
Facebook messenger	5.38	2m46s	Torrent	109	3m40s
Yahoo messenger	0.56	2m6s	Yahoo text chat	0.55	3m52s
Skype 7.2.2	4.88	5m	Online gaming	3m	9m5s
Viber	1.04	1m42s	Youtube	7.55	1m39s
Non-VoIP			Antivirus update	1.85	1m20s
Download manager/FTP	65	5min	Mixed Non VoIP	46	13m39s
Web Browsing	2.37	2m52s	Mixed VoIP and Non VoIP	9.28	5min

Table 7: Own captured VoIP and non-VoIP traffic traces for performance evaluation

5.3 Accuracy

We evaluated our system for accuracy. We considered the typical parameters used for measuring accuracy. These parameters are

- DR (Detection Rate): How many VoIP flows are correctly identified?
- FPR(False Positive Rate): Measure of flows incorrectly identified as VoIP
- TP (True positive): Measure of flows correctly identified as VoIP.
- FN(False Negative): Measure of flows that are incorrectly identified as Non-VoIP
- TN(True Negative): Measure of flow correctly identified as Non VoIP.

We calculated the DR and FP for different traces obtained from tstat, wireshark site and own VoIP and Non VoIP setups.

The accuracy is calculated by the expression

$$\text{Accuracy (DR)} = \frac{TP}{TP+FN} \times 100\% \quad \text{(Eq. 1)}$$

$$\text{FPR} = \frac{FP}{FP+TN} \times 100\% \quad \text{(Eq. 2)}$$

Total flows shows the total number flows in given data set. As discussed earlier, the system can only identify flow as VoIP or Non-VoIP if it is of duration equalvalent or above than 5 seconds or of 100 packets. In the data set of codec G729, 5 flows are detected but 2 of them has duration of beyond 5seconds. The system correctly identify it a VoIP flow. In Skype dataset, out of 48 flows only 2 are beyond 5 seconds.Table 8 and 9 shows the accuracy and efficiency of the proposed system for rest of datasets.

5.4 Efficiency

We evaluated system efficiency in terms Average numbers of packets processed by our system per second and execution time. The average VoIP detection time for Voice traffic is less than 7 seconds.

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

Trace	Codec	Total Flows	TP	FP	Accuracy (DR)	FPR	Avg. packets processed/sec	Execution Time
E2E-140606-1	G729	5	2	0	100%	0.0%	22550.25	4sec
E2E-140606-1	iLBC	3	2	0	100%	0.0%	33391.66	3sec
	iSAC	2	2	0	100%	0.0%	24591.00	3sec
SkypeOut-260906-tcp	G729	4	2	0	100%	0.0%	22831.50	4sec
SkypeOut-260906-udp	G729	4	2	0	100%	0.0%	18468.80	5sec
Internet-E2X-29		20314	43	22	66%	33.8%	32301.32	1m15sec
Accuracy on tstat traces					94.33%	5.63%		

Table 8: Accuracy and efficiency w.r.t tstat traffic traces

VoIP Applications tested	Total flows	TP	FP	Accuracy	FPR	Average packets processed	Execution time
Google hangouts	2	2	0	100%	0%	15200	1sec
Facebook messenger	4	2	0	100%	0%	4104.0	1sec
Yahoo messenger	13	2	0	100%	0%	5200	1sec
Skype 7.2.2	48	2	0	100%	0%	32964.0	1sec
Viber	2	2	0	100%	0%	7322.0	1sec

Table 9: Accuracy and efficiency for own captured VoIP traffic traces

5.5 Scalability

We tested most familiar VoIP applications and detected VoIP traffic traces with high accuracy and efficiency. The proposed solution is generic and hence can detect VoIP flows regardless of application, protocol, codec used and security mechanism. The system can be implemented at one-way or two way network interface.Our system is only specific to VoIP detection so it has better results thanother P2P traffic classifiers. So our system is scalable and practically implementable at telecommunication authorities or ISPs gateway with powerful servers and optimized and efficient programming implementation for realtime VoIP calls detection.

6 Conclusion and Future Work

In this paper we purposed a joint port and statistical analysis-based hybrid approach to detect encrypted, un-encrypted and tunneled VoIP and Non VoIP flows. We tested most common VoIP and non-VoIP applications and services and evaluated our system for accuracy, efficiency and scalability. Result shows that our system can detect VoIP flow with an accuracy of 97.165%. It is useless to detect VoIP flows after the communication has ended. Despite of calculating statistical values for the whole communication we focused on sliding window approach. Our system calculates statistical parameters for 5 seconds of the flow or only first 100 packets are analyzed to get threshold values. Our system can successfully detect VoIP within 6 seconds of communication. The proposed system is

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

generic, fast, and practically implementable which can be used to detect VoIP flows generated by any VoIP application. It can maintain validity when existing VoIP applications are updated or new ones admitted. It is best choice for ISPs, telecommunication authorities and law enforcement agencies to prioritize, block and for surveillance of VoIP traffic.

References

1. Leung, C.-M. and Y.-Y. Chan. *Network forensic on encrypted peer-to-peer voip traffics and the detection, blocking, and prioritization of skype traffics*. in *Enabling Technologies: Infrastructure for Collaborative Enterprises, 2007. WETICE 2007. 16th IEEE International Workshops on*. 2007. IEEE.
2. Renals, P. and G.A. Jacoby. *Blocking skype through deep packet inspection*. in *System Sciences, 2009. HICSS'09. 42nd Hawaii International Conference on*. 2009. IEEE.
3. Risso, F.G.O., et al., *Lightweight, payload-based traffic classification: An experimental evaluation.* 2008.
4. Lu, F., X.-L. Liu, and Z.-N. Ma. *Research on the characteristics and blocking realization of Skype protocol*. in *Electrical and Control Engineering (ICECE), 2010 International Conference on*. 2010. IEEE.
5. Ehlert, S., et al., *Analysis and signature of Skype VoIP session traffic.* 4th IASTED International, 2006.
6. Baset, S.A. and H. Schulzrinne, *An analysis of the skype peer-to-peer internet telephony protocol.* arXiv preprint cs/0412017, 2004.
7. Anwar, U., G. Shabbir, and M.A. Ali, *Data Analysis and Summarization to Detect Illegal VOIP Traffic with Call Detail Records.*International Journal of Computer Applications, 2014. **89**(8): p. 1-7.
8. Lin, Y.-D., et al., *Application classification using packet size distribution and port association.* Journal of Network and Computer Applications, 2009. **32**(5): p. 1023-1030.
9. Zuev, D. and A.W. Moore, *Traffic classification using a statistical approach*, in *Passive and Active Network Measurement*. 2005, Springer. p. 321-324.
10. Yildirim, T. and P. Radcliffe. *A framework for tunneled traffic analysis*. in *Advanced Communication Technology (ICACT), 2010 The 12th International Conference on*. 2010. IEEE.
11. Khan, F.I.U.A., *A generic technique for voice over internet protocol (VoIP) traffic detection.* IJCSNS, 2008. **8**(2): p. 52.
12. Freire, E.P., A. Ziviani, and R.M. Salles, *Detecting VoIP calls hidden in web traffic.* Network and Service Management, IEEE Transactions on, 2008. **5**(4): p. 204-214.
13. Freire, E.P., A. Ziviani, and R.M. Salles. *Detecting skype flows in web traffic*. in *Network Operations and Management Symposium, 2008. NOMS 2008. IEEE*. 2008. IEEE.
14. Crotti, M., et al. *A statistical approach to IP-level classification of network traffic*. in *Communications, 2006. ICC'06. IEEE International Conference on*. 2006. IEEE.
15. Okabe, T., T. Kitamura, and T. Shizuno. *Statistical traffic identification method based on flow-level behavior for fair VoIP service*. in *VoIP Management and Security, 2006. 1st IEEE Workshop on*. 2006. IEEE.
16. Piskac, P. and J. Novotny, *Using of time characteristics in data flow for traffic classification*, in *Managing the Dynamics of Networks and Services*. 2011, Springer. p. 173-176.
17. Korczynski, M. and A. Duda. *Classifying service flows in the encrypted Skype traffic*. in *Communications (ICC), 2012 IEEE International Conference on*. 2012. IEEE.
18. Zander, S., T. Nguyen, and G. Armitage. *Automated traffic classification and application identification using machine learning*. in *Local Computer Networks, 2005. 30th Anniversary. The IEEE Conference on*. 2005. IEEE.
19. Nguyen, T.T. and G. Armitage, *A survey of techniques for internet traffic classification using machine learning.* Communications Surveys & Tutorials, IEEE, 2008. **10**(4): p. 56-76.

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

20. Alshammari, R. and A.N. Zincir-Heywood, *How Robust Can a Machine Learning Approach Be for Classifying Encrypted VoIP?* Journal of Network and Systems Management, 2014: p. 1-40.
21. Alshammari, R. and A.N. Zincir-Heywood, *Identification of VoIP encrypted traffic using a machine learning approach.* Journal of King Saud University-Computer and Information Sciences, 2015.
22. McGregor, A., et al., *Flow clustering using machine learning techniques*, in *Passive and Active Network Measurement*. 2004, Springer. p. 205-214.
23. Gómez Sena, G. and P. Belzarena. *Early traffic classification using support vector machines*. in *Proceedings of the 5th International Latin American Networking Conference*. 2009. ACM.
24. Gowsalya, R.A. and S.M.J. Amali, *SVM Based Network Traffic Classification Using Correlation Information.* Networking and Communication Engineering, 2014. **6**(5): p. 188-192.
25. Alshammari, R. and A.N. Zincir-Heywood, *Can encrypted traffic be identified without port numbers, IP addresses and payload inspection?* Computer networks, 2011. **55**(6): p. 1326-1350.
26. Alshammari, R. and A.N. Zincir-Heywood. *An investigation on the identification of VoIP traffic: Case study on Gtalk and Skype*. in *Network and Service Management (CNSM), 2010 International Conference on*. 2010. IEEE.
27. Do, L.H. and P. Branch, *Real time VoIP traffic classification.* Techni-cal Report 090914AIR].[S. 1.]: CAIA, 2009.
28. Adami, D., et al., *Skype-Hunter: A real-time system for the detection and classification of Skype traffic.* International Journal of Communication Systems, 2012. **25**(3): p. 386-403.
29. Adami, D., et al., *A real-time algorithm for skype traffic detection and classification*, in *Smart Spaces and Next Generation Wired/Wireless Networking*. 2009, Springer. p. 168-179.
30. Birke, R., et al., *Experiences of VoIP traffic monitoring in a commercial ISP.* International Journal of Network Management, 2010. **20**(5): p. 339-359.
31. Birke, R., et al. *Understanding VoIP from backbone measurements*. in *INFOCOM 2007. 26th IEEE International Conference on Computer Communications. IEEE*. 2007. IEEE.
32. IPSec, http://en.wikipedia.org/wiki/IPsec#Transport_mode
33. Skype Traces,http://tstat.tlc.polito.it/traces-skype.shtml
34. Sample VoIP and non-VoIP traffic traces, http://wiki.wireshark.org/SampleCaptures

https://sites.google.com/site/ijcsis/
ISSN 1947-5500