Journal of Computer Networks, 2013, Vol. 1, No. 2, 15-27
Available online at http://pubs.sciepub.com/jcn/1/2/1
© Science and Education Publishing
DOI:10.12691/jcn-1-2-1

Identification of Hidden VoIP (Grey Traffic)

Ch. M. Asim Rasheed[1], Ayesha Khaliq[1], Ammara Sajid[1], Sana Ajmal[2,*]

[1]National University of Science and Technology, Pakistan
[2]Centre for Advanced Studies in Engineering, Pakistan
*Corresponding author: sana.ajmal84@yahoo.com

Received December 18, 2012; Revised May 10, 2013; Accepted May 12, 2013

Abstract National Telecommunication Regulator in many countries around the world imposes call termination taxes on national calls as well as international calls landing in that country. In many third world countries, every year up to 90 % of the international traffic bypasses regulatory checks, causing a huge revenue loss to the country. The use of illegal gateways to bypass the Voice Clearing Houses to terminate international traffic using VoIP gateways, GSM / local line branch exchanges or other related equipment are the simplest means of Grey traffic. Use of the encryption and other network design techniques are the easiest methods to hide the VoIP traffic from any clearing house. We have proposed an architecture based on a mathematical model to detect, segregate and qualify VoIP traffic (Grey) into different categories. The proposed model identifies grey traffic, through traffic analysis techniques coupled with statistical anomaly based intrusion detection system and behavior analysis.

Keywords: *voice over internet protocol (VoIP), grey traffic, international clearing house (ICH), intrusion detection system (IDS), statistical analysis*

1. Introduction

The debate for segregation of privacy and security is taking momentum since long. However the bleak line segregating both is a tricky issue and varies from society to society. In many societies, any kind of data sharing between two legitimate users is considered as personal issue. A lot of research has been done to hide the personal commercial or non commercial data over the Internet. Data de-shaping techniques [1], such as encryption, passing through distributed ingress routes and tunneling are the common and widely used techniques to keep privacy of the data. However, due to increased cyber attacks and strict regulatory policies in many countries, have initiated a serious debate to re-define the upper limit of privacy. A policy like PIPA [2] is another outcome of this controversial debate.

Grey traffic is a prevalent problem regarding landing of illegal voice traffic over the Internet. This incurs substantial monetary losses not only to the operators and the private telecommunication companies but also to the state [3]. Illegal commercial VoIP traffic bypasses regulatory checks by disguising it. As, the grey traffic cannot be detected at the clearing points; hence the taxes are evaded [4]. Combination of multiple techniques with the encryption, aides in masking of the VoIP traffic as normal data traffic. Such techniques force regulatory checks to let it through without applying taxes [5]. In many cases, de-shaping absolutely changes the behavior or pattern of the traffic. This adds more complication to the situation.

This is the basis of our study which identifies and detects de-shaped VoIP traffic over the Internet. We observed the behavioral patterns being followed y the VoIP traffic over the Internet. We created a profile for standard VoIP flow and applied it to detect grey traffic. Pattern matching was conducted for Internet traffic against the statistical profiles, for further categorization basing on the match factor. Based on the profile matching, an Intrusion Detection System is proposed that detects encrypted VoIP traffic over the Internet through probabilistic estimation [6].

This paper proposes a technique to detect Grey VoIP traffic along with detection of encryption type and encryption layer. We were able to incorporate the proprietary protocols detection. Without going in to decryption and deep packet analyses, our approach established the VoIP traffic patterns. These patterns were used to detect anomalies in network traffic to segregate and qualify VoIP traffic into different categories. Using modular design, we propose a technique to capture packets from different routers. By combining the collected information, offline analysis was carried out. In some cases, by using flow behavior, we were even able to guess particular voice codec being applied.

The rest of the paper is organized as follow; Section II discusses the specifications of Grey VoIP traffic. Section III explains intrusion detection techniques for VoIP including proposed approach. Section IV discusses results and evaluation of the proposed approach. Section V concludes the paper.

2. Characteristics of Grey VoIP Traffic

The introduction of VoIP helped in development of many commercial and non commercial applications over the Internet. Non commercial VoIP services such as point to point or multipoint chat or conference services are considered legitimate and legal in almost all countries of the world. However, the problem started when users started commercial VoIP services incorporating third party transit or termination points. The simplest example of such models is use of Skype [7] like services for voice termination over the public switched networks.

Introduction of VoIP traffic introduced a major changeover for voice based telephony, especially for revenue of the telecommunication operator operators. In pre-VoIP world, the voice data flows were generally computed according to duration of session, rather than on volume basis. Introduction of VoIP allowed telecommunication operators to share and transit voice data on volume basis disregard of its duration. This concept provided significant growth in telecommunication sector, especially for long distance and international calls. The growth of the telecommunication sector created opportunity for the telecommunication operators to reduce their operational expenditures by reducing interconnects cost. The reduction in the transit rates and the operator to operator interconnect rates allowed enhanced revenues for the operators. However, at the same time, the regulatory authorities considered clear definition of the interconnect and transit rates. Such definition helps to avoid monopolization, revenue assurance and fairness for all operators in the market.

The state agencies involved in the implementation of the taxes over the telecommunication operators have installed International Clearing Houses (ICH), especially for the VoIP traffic. Role of clearing house is to segregate the VoIP traffic from the normal Internet non VoIP traffic. It also includes determination of the operators involved in the traffic handling and to apply the taxes accordingly. The clearing houses are generally deployed at the data ingress points such as international data landing stations to monitor entire traffic entering through the path. Filtering techniques are subsequently applied on the ingress traffic to determine the source, destination and total data volume of the VoIP traffic for calculation of taxes. Similar to custom duties on the imported items, many regulatory authorities also consider the incoming international commercial VoIP as “imported voice” hence applies special taxes [3].

At one end, these regulations have created new business opportunities for provision of third party transit and interconnect services. On the other hand, these regulations have allowed the data operators and the Internet service providers (ISP) to illegally handle VoIP traffic. By avoiding regulatory checks, these operators provide same services at substantially lower cost than legal operators [3].

The VoIP de-shaping techniques allow illegal operators, such as Grey traffic handlers, to easily manipulate VoIP traffic flow [3,4]. The evaded taxes not only hamper the national income but also telecommunication growth of the specific country. As one party involves in such activities remains outside national boundaries, hence the legal action against such parties remain quite tricky and expensive option. This limitation allows foreign end of the illegal operators to open multiple parallel channels with the single or multiple illegal local operators. Due to involvement of huge illegal revenues, options for such operators remain open to install high end routers and combination of VoIP de-shaping techniques.

2.1. Plain VoIP Traffic

The VoIP traffic in plain and grey mode behaves significantly different for any clearing house. For a plain and a legitimate encrypted VoIP traffic, many well defined architectures and protocols has been defined over the years, by the researcher community. Without going to the details, many standardization agencies like the International Telecommunication Union (ITU) etc have presented a number of VoIP protocols and architectures, such as:

- H.323
- IP Multimedia Subsystem (IMS)
- Media Gateway Control Protocol (MGCP)
- Session Initiation Protocol (SIP)
- Real-time Transport Protocol (RTP)
- Session Description Protocol (SDP)
- Inter-Asterisk eXchange (IAX)
- Skype Protocol
- Skinny Call Control Protocol (SCCP)

Out of above mentioned protocols, H.323, Session Initiation Protocol and Real-time Transport Protocol gained large scale popularity among the telecommunication operators [8]. One of the significance of all these architectures is the segregation of the control and the data flows over the Internet. In all these protocols, the control traffic is a distinct characteristic for the determination of involved IP addresses and other flow statistics.

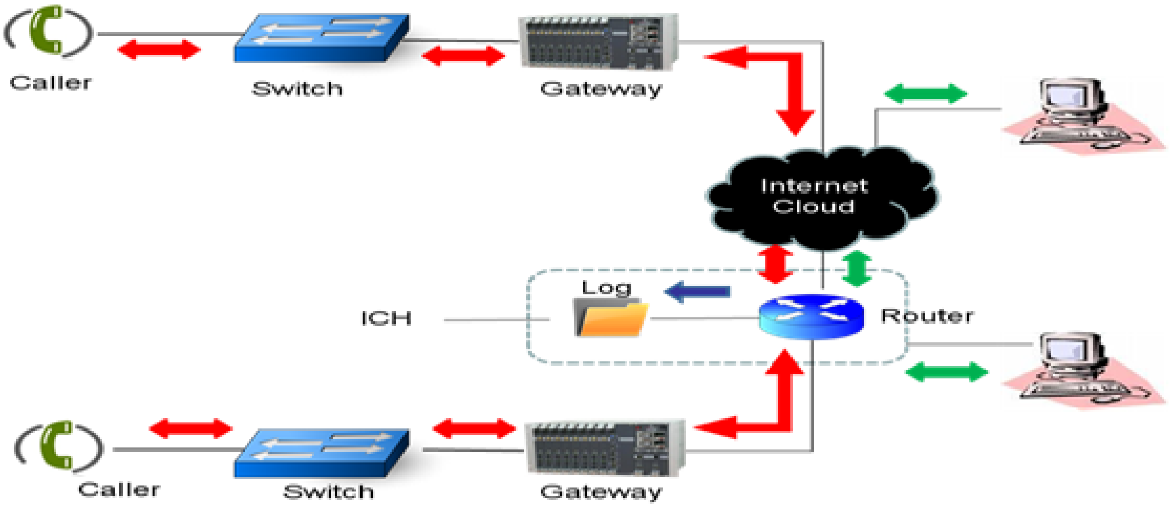


Figure 1. Normal VoIP Flow

For determination of standard VoIP traffic, one can assume a simple but standard scenario. As a standard case, clearing house is deployed at the ingress router as described in Figure 1. The landing Internet data which contains standard (plain) and encrypted Internet traffic including VoIP. Clearing house observes the VoIP traffic signatures against normal non VoIP Internet data traffic. This is done by matching VoIP control traffic against specific VoIP protocol [9]. VoIP statistics are determined for post processing of VoIP flow according to regulatory policies.

For advanced level of the clearing houses, the VoIP control traffic is compared against the VoIP data traffic for correct estimation of traffic. However, this approach involves significantly high filtering resources at the ingress routers. Moreover, to avoid processing delays, such detailed analysis is not implemented at all clearing houses. Such limitation provides opportunity to the grey traffic handlers to simply hide the control traffic to bypass the clearing house.

2.2. Grey VoIP Traffic

The target of grey traffickers is to bypass clearing house, hence evade taxes. The easiest way to bypass clearing house is through de-shaping VoIP signatures. Due to involvement of huge revenues, research is also involved at grey traffickers end as well to introduce new clearing house bypassing techniques [10]. The evolutionary process in development of traffic de-shaping techniques passed through many phases as under:

2.2.1. Isolated Data Links

Use of the isolated data links for the VoIP control traffic [5,10,14] from other VoIP data was considered as the simplest method to hide the control information. As most of the clearing houses are intended to compute the voice statistics, rather than analyzing the voice contents. Such clearing houses are more concerned with the VoIP control traffic than the data traffic. By design, the VoIP control traffic requires lesser bandwidth as compared to the data traffic. Hence, it can be bypassed from clearing house using isolated channels. Use of satellite links is the simplest and most effective method in this regard.

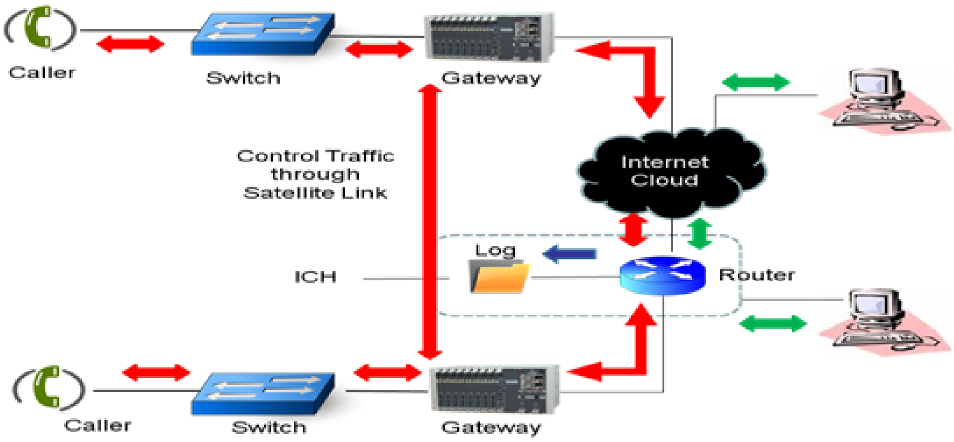


Figure 2. Isolated Control Traffic VoIP Flow

Figure 2 depicts the flow of the isolated control traffic between VoIP gateways using the satellite links. As the satellite links bypasses the clearing house, it fails to detect actual amount of the voice calls flow. Resultantly, such scenario causes false statistics by the clearing house.

2.2.2. Control Traffic Manipulation

The manipulation of the control traffic of any VoIP protocol was considered as initial effort [11] for the grey traffic introduction. Other than using isolated channels for VoIP control traffic, the grey traffickers used simple encryption techniques to hide the control traffic passing through clearing house. Resultantly the clearing houses involved in the data acquisition through control overheads, failed to acquire the statistics. This technique introduced minimum overheads for overall traffic. However, this approach could easily be compromised by the detailed data traffic analysis.

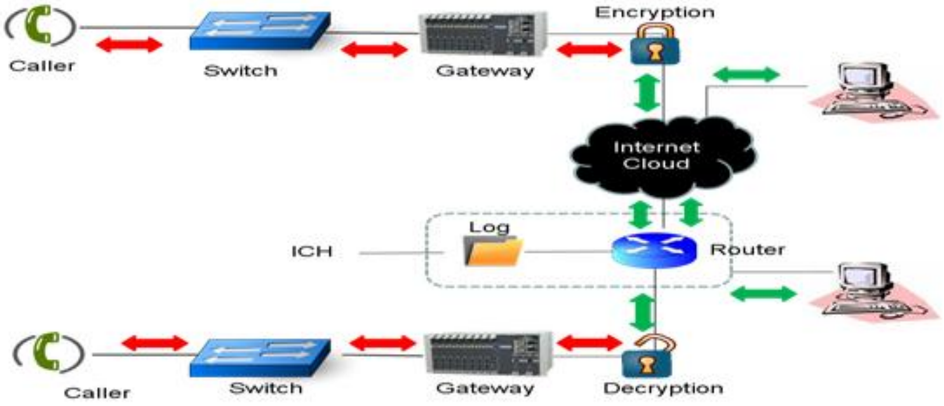


Figure 3. Encrypted VoIP Flow

2.2.3. Continuous Traffic

Many organizations like financial institutes, health managers, or even a few public sector institutes use continuous encrypted traffic for their routine functionalities. A large scale of data communication is based on the end-to-end or router-to-router encryption [13]. Hence, use of the encryption is the easiest method to de-shape any data signatures [10,12]. For the grey traffic, the VoIP control or even data traffic is encrypted before entering the Internet cloud. The encrypted traffic is then decrypted after the clearing house. The end to end encryption of the VoIP data traffic along with the VoIP control traffic could merge the VoIP signatures with the other encrypted traffic over the Internet. The flow is decrypted in Figure 3, where clearing house detecting the VoIP protocol, is unable to segregate normal data and encrypted VoIP traffic. This approach made job of the clearing house, quite complicated. However, the regulators managed to cope up the issue through statistical analysis of over all traffic [15] as described in subsections.

2.2.4. Multiple Simultaneous Flows

Use of multiple simultaneous uni-directional traffic flow [10,12,14] is the third modification in the chain. Most of the countries or networks have more than one data traffic landing stations. Use of separate ingress and egress paths for the entering and leaving VoIP traffic could easily make the statistical analysis quite complicated. This approach gives incomplete and partial data for the statistical analysis. Using this approach can easily force the clearing house to generate true alarms for all channels or data flows. Due to the nature of this approach, a clearing house may have to process a large chunk of the data without getting the true picture.

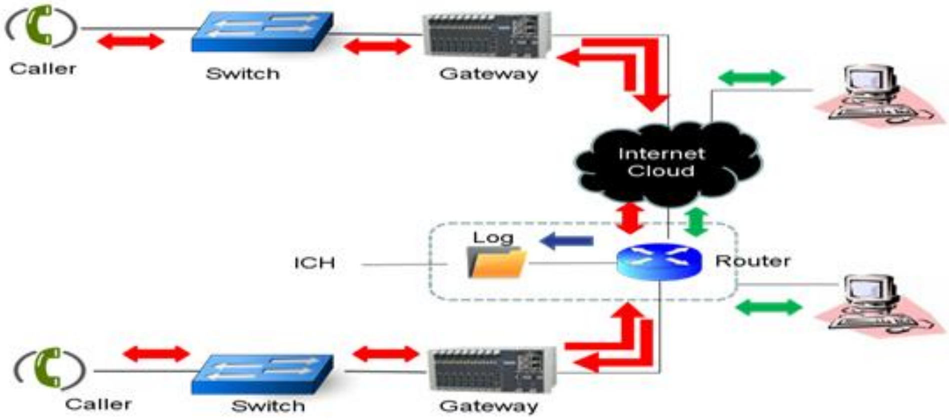


Figure 4. Multiple uni-directional VoIP Flow

Figure 4 depicts the simultaneous multipath flows for VoIP traffic. The entire data traffic is passing through the network connected with the clearing house. However, involvement of different IP addresses and segregated routes, make the flow analyses quite complicated for large scale data flows, e.g. multiple terabytes per second.

2.2.5. Hybrid Approach

Use of the hybrid mechanism is the most complex design adapted by the grey traffickers. This technique involves use of all or combination of the above mentioned schemes, i.e. encryption, multiple uni-directional flow and isolation of control traffic. Large amount of the revenue involved in the grey traffic business lure the criminals to invest heavily in the business. Use of fast processing machines, to avoid degradation in call quality can easily be introduced by the grey traffickers. Use of the proprietary encryption techniques, isolated satellite links and fast processing end routers, could easily be deployed to earn large revenues.

In our design, we intend to develop an approach which could target the hybrid approach.

3. Intrusion Detection for VoIP Traffic

Due to involvement of encryption and other complicated traffic de-shaping techniques, guaranteed identification of grey traffic is always questionable. Although, considering this limitation, one can argue on the end goal of the entire proposed approach. Resultantly, the main goal of the proposed approach is not to charge the grey traffic according to regulatory regime. Rather, the aim is to identify the grey traffickers for subsequent legal action. The grey traffic in many countries is considered as illegal and a violation of law. Hence, identification of end hosts involved in grey traffic can significantly assist law enforcement agencies to arrest the culprit and initiate legal proceedings.

Although, subsequent steps towards authentic determination of grey traffic are beyond scope of this paper. However, for better understanding of end goal, a brief discussion in this regard is done in subsequent paragraphs.

To bypass ICH for transfer of grey traffic is not fruitful, till it is terminated appropriately at the end users. For smooth termination of grey traffic, transfer of traffic to some legal telecommunication operator is required. Hence we can divide the grey traffickers in different categories, as:

- The legal operators can terminate the grey traffic relatively easily, especially within their own network. However, inter operator traffic reconciliation and can assist in this regard.
- Traffic handling by the non operators need interfacing with the legal operators for termination of traffic. The technical approach coupled with other techniques can help the regulatory agencies in reduction of overall grey traffic. Other techniques, such as physical checks, determination of terminal telephone lines,

variation in traffic load on cellular Base Transceiver Stations (BTS) and source number analysis, etc, can greatly assist towards the end goal.

- Use of encrypted tunnels can hide the end users. However, determination of tunnel end point routers can itself lead towards the grey trafficker.

The threats and challenges posed by the grey traffickers required new research to answer the issue in highly professional manner. There are many techniques proposed for the intrusion detection systems (IDS) and traffic & signature analyses especially for VoIP traffic [6,15,16]. Comparison of different schemes is as under:

3.1. Current Approaches

Network monitors can help in managing the networks, logging network activity and creating history reports [24]. However, network monitors do not use profile based matching to detect any certain type of the traffic. The variety of the attacks and increased sizes of the attack signatures, make the task of IDS quite complicated. Hence, the forensic process must inspect the traces against all the attacks and the fingerprints. Due to variety of the applications and the type of attacks at different layers, the pattern of intruders is not localized to the specific packet. This limitation demands analyses of the each packet, against the attacker signatures.

Packet sniffers like Wireshark [21] can capture the packets and examine their headers to log the relevant information of the passing traffic. These packet analyzers only work on the standard protocols. Packet sniffers are generally packet-centric (not data-centric). They do not provide the analysis of the overall end-to-end flow or the applications in use. Such analyzers operate on per packet basis, as they generally do not give information of sessions and type of flows [21].

Deep packet analyzers (DPA), e.g. SNORT [22] examines the data part of the packet by decoding it. They detect protocol viruses, worms and intrusion for the purpose of collecting statistical information. However, use of the encryption or the distributed data flow paths complicates the job of the DPA.

Other than the open market IDS and DPA tools, researchers have made other endeavors to answer the challenge. The efforts were generally made for a specific network design or architecture. A very few contributions were made purely for a large sized and multi-interface network such as national Internet architecture. Moreover, the IDS or the DPA, specifically for the grey traffic handling are rarely used. Serious efforts have been made by the researchers to detect VoIP from the tunnels. Similarly, different VoIP protocols have been targeted for the detailed analysis.

Statistical analysis is considered to be a suitable approach for the VoIP detection through encrypted tunnels [16,23]. Statistical finger printing or analysis is also proposed for the detection of any specific protocol [15]. Detection of the transport layer protocol like UDP, TCP, SSL or TLS and application layer protocols like FTP or HTTP can be detected by using statistical or behavior analysis. However, statistical analysis demands availability of the entire data statistics before performing classification. This limitation makes the overall requirement of the classifier, quite complicated. Similarly, end-to-end encrypted tunnel at the network layer, poses complicated challenge for the detection of the application layer protocols.

The idea to perform distributed IDS is not new. Many researchers [17,18,19,20] have proposed multiple schemes to cater different type of challenges. These challenges involve distributed data sets and encryption. However, the verification of a composite model for the large scale national level networks, still remain a practical challenge. Involvements of the proprietary or multi-layered encryption with distributed data sets make the situation more complex. Due to this very reason, a dire need was felt to develop a comprehensive model specifically for the VoIP grey traffic.

3.2. Proposed Approach

We observed that even after a lot of the dedicated effort by the researchers, no single approach could answer all the challenges, as:

- Deep packet analyzers are generally slow in performance. Hence, the DPA of large sized or national level network can cause bottle neck for the overall network traffic.
- Offline DPA processing of any network traffic can eliminate the choking problem. However huge memory banks will be required to capture and save the complete network traffic.
- DPA processing for multipoint ingress for VoIP traffic needs convergence of the entire data flow, to link two way traffic flows for same VoIP sessions.
- Use of distributed network paths can limit the performance of statistical analyzer. Hence deployment of the large size IDS at all data entry points may become a financial restriction.
- Use of the encryption at lower layers (e.g. IPSec or PPtP) makes equal sized packets to traverse the network. Resultantly, the statistical analysis of the upper layers gets complicated.
- For the encrypted grey traffic, determination of number of concurrent sessions remains unavailable. Even use partial statistical analysis according to packet arrival time variations cannot help in this regard.
- Use of proprietary voice codec and encryption protocols may substantially change the traffic signatures. This limitation deprives complete automation and demands manual observation and intervention for the runtime analysis.
- The grey traffickers may periodically change source and destination IP addresses. Counter technique to this approach needs continuous liking of historical data, as well as determination of physical address of source / destination.

3.3. Design.

The analysis of these limitations needs a generic architecture duly linked with the human intelligence for the runtime routines. We considered application independent approach using detailed behavior and statistical analysis. The proposed approach can be deployed through the distributed architecture, using modular approach. The distributed and the modular design allow further detection and classification in the layered methodology.

This paper proposes a solution, consisting multiple stand-alone modules for detection of encrypted packets over the Internet. To use the previous research and to target the overall solution, we propose aggregation and combination of a few previously proposed approaches. The aggregation under the modular architecture proved to be more promising and realistic. Combining the best proposed solutions under one platform may create interoperable issues; however, a well defined and implemented design can offer smooth operations.

For the final analysis, behavior of the captured traffic over a period of time is analyzed for the subsequent categorization. We considered use of the different traffic analysis techniques defined for the VoIP and non VoIP analysis. We also considered a simplified model based on pattern and behavior analysis of the non grey VoIP traffic. We propose an approach for the VoIP detection, based on the combination of best effort techniques to address the issue as following:

- *Modular deployment*. Deployment of the overall system under different stand alone modules offers maximum flexibility. This approach also allows modification or up-gradation of any module without affecting the network or VoIP detector efficiency. We propose four different modules in this regard. The detail of the each proposed modules is explained in subsequent paragraphs.
- *Mirroring traffic at ingress / egress router of the network*. We propose to create a parallel link at each ingress and egress router. Mirroring of traffic flow will allow smoothness of overall Internet traffic. Any delay or malfunction will only affect the VoIP analysis without affecting the normal data or even under analysis VoIP traffic.
- *Extraction of packet features for statistical analysis*. Instead of performing DPA, we observed use of the statistical and behavioral analysis more suitable for the task. This approach follows extraction of detailed information through the packet header analysis. The small sized extracted header fields will act as input for the subsequent processing.
- *Short-listing packets of interest*. The overall analysis of any national Internet traffic [23] proves that VoIP consumes limited chunk of resources as compared to over all data traffic. Hence the total size of processed data can be reduced significantly by discarding the non-VoIP and plain VoIP data.
- *Logical packet and session processing*. The outcome of each packet can be made useful for the final analysis, if session information is acquired through the post processing of extracted header information. This step can be quite time consuming due to involvement of the large sized historical data processing. To reduce the processing time, this step may involve use of the refined and parallel database.
- *Pattern matching*. Pattern analysis of the captured traffic with the standard observed VoIP traffic patterns is the most important process of the overall system design. This step involves intelligent behavioral and statistical analysis coupled with the human intelligence. The rules according to historical data analysis need to be updated on regular interval for improved efficiency of the system.
- *Classification of suspected IP addresses*. This is the last step of the proposed system. The suspected traffic can be classified as highly, moderate or slightly suspicious basing on the rule matching of the previous step.

3.4. High Level Architecture

The proposed model is deployable in four standalone but inter linked modules. Each previous module will act as input to subsequent module. For the ease of deployment, we considered that out of all four modules, only the first module needs to be deployed at each data ingress / egress point. For the better efficiency, this module can be deployed at national ingress router at ICH. This will cater analysis of entire traffic entering and leaving the network with minimum resource deployment. The remaining three modules can be deployed at any central location.

Deployment of capturing module at national ingress point (ICH) will allow monitoring of entire data traffic entering the country. Although, such requirement can create a bottle neck and may require significant processing resources. However, as the ICHs are already processing the entire Internet traffic, the deployment of first module will not add any significant processing delay for the traffic. Moreover, considering the revenue loss involve in handling of the grey traffic, one time expenditure and proper offline configurations can significantly help towards resolution of the problem.

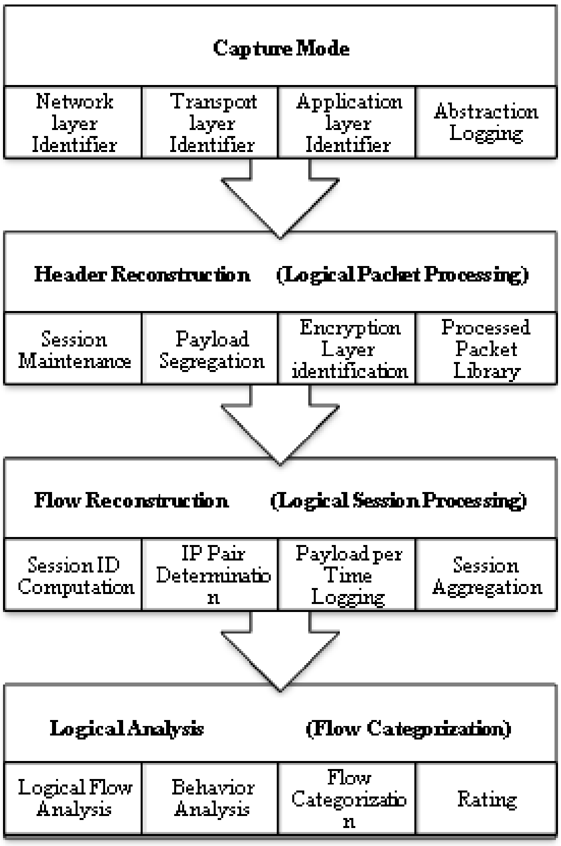


Figure 5. Proposed Flow

The ICH installed at national traffic ingress points already performs traffic determination process for standard VoIP traffic. Hence installation of module 1 at such routers will not add significant overhead.

In addition to ICH, module 1 can also be deployed at public sector ISPs, which enjoy significant market player (SMP) status. Such ISPs are considered trusted ISPs, and work directly under public sector entities. Deployment of module 1 in such circumstances will provide distributed deployment and more flexibility.

Module 2, 3 & 4, which are actually more complicated and require high processing, can be installed as standalone machines. These three modules will use data provided by module 1, hence will not affect runtime traffic.

High level architecture with proposed flow for all of the modules is shown in Figure 5.

3.4.1. Capture Mode

This is the first module proposed in the list. This is the only module which needs to be working on the runtime. This module captures entire mirrored traffic from each of the ingress and egress routers within any network. The captured traffic is used for the extraction of the multi-layer packet header information. Twenty three different header values are extracted from the top four layers of TCP/IP stack. However, in case of the encrypted traffic, information related to all of the fields may not be available.

Starting from the MAC layer, subsequent top layers may not provide sufficient information due to encryption at different layers. Regardless of the type, the header information in each packet from the highest accessible layer is scanned. To avoid the packet loss which may lead to false alarm, all of the packets are treated in similar way without any post processing. However, redundant data could be eliminated in subsequent modules through virtually offline filtering. By using the capture mode, following useful and relevant fields can be extracted depending on the type of encryption used:

- Packet Arrival Time
- Header Size (Data Link Layer)
- Payload Size (Data Link Layer)
- Protocol Type (Network Layer)
- Payload Size (Network Layer)
- Header Size (Network Layer)
- Source IP (Network Layer)
- Destination IP (Network Layer)
- Next Protocol (Network Layer)
- Next Protocol Header (Network Layer)
- Next Protocol Payload (Network Layer)
- Next Protocol Type (Network Layer)
- Transport Protocol (Transport Layer)
- Source Port (Transport Layer)
- Destination Port (Transport Layer)
- Payload Size (Transport Layer)
- Header Size (Transport Layer)
- Sequence Number (Transport Layer Encryption)
- Acknowledge Number (Transport Layer Encryption)
- Application Protocol (Application Layer)
- Payload Size (Application Layer)
- Header Size (Application Layer)
- Application Reserved (for application layer proprietary protocols).

The output of capture mode can be logged for extraction of session and flow information. The extracted information from each ingress / egress router can be maintained at some central server for minimal deployment. The same information will act as input to the next module. Different “Raw” files extracted through multiple bidirectional or unidirectional flows at same or different timings can be analyzed simultaneously for combined output. This approach will not only cater entire network traffic, but will also counter distributed flows used for the de-shaped VoIP traffic.

3.4.2. Header Reconstruction

This is the second proposed module of the chain. This module can either be deployed independently or in conjunction with the third module. The aim of this module is to develop the process packet library (PPL) from the raw packet library. The PPL will establish transport layer session information of each packet. For every entry in the raw library, this module will check the source and destination IP address and port numbers. It will log payload size based upon the sessions. For any new port which is different from the ports of the previous entries, the entry is considered to be a new session between an IP address pair. For every new session, the number of sessions between an IP pair will increment linearly. For each session, the total payload size and the duration of the session are re-computed. Also, the encryption layer on the packet is determined basing on the last accessed header. The PPL as output of Module-2 will contain minimal data set entries including:

- Source and Destination IP.
- Source and Destination port.
- Session Start and End Time.
- Encryption layer.

3.4.3. Flow Reconstruction

The third module for the logical session processing (LSP) is the most time consuming part of the design. The PPL database includes entire traffic entries. The LSP constructs the end-to-end session information from the PPL. The packet arrival time for different sessions may not follow the same behavior. Hence, the session maintenance will require search from entire PPL database. For the each IP pair, identified in PPL, LSP will create a pair of database entries for each direction of traffic flow. Assuming, if the IP pair is “A” & “B”, then two separate databases will be created, one for traffic flow from “A” to “B” and the other for “B” to “A”. This approach will help to determine the bi-directional flow behavior of the VoIP traffic at distributed network paths.

Due to involvement of heavy processing, we recommend use of professional database (e.g. MySQL or Oracle etc). The resultant output database entries will contain all the sessions between an IP pair, encryption layer and the payload for each session logged against time. To draw the time based graph, the output database will be updated periodically according to the change status of the payload, number of sessions or time.

This approach can manipulate the processed data for analysis purpose. Different sessions of the same IP pair may start and end at different times. The LSP can maintain different database graphs for the payload, number of sessions, etc, against time. This can help in the computations regarding session durations and number of sessions maintained during a time interval for the post analysis. The output of this module is recorded as the Processed Session Library (PSL). The PSL will act as raw data for the logical analysis in classification of data traffic.

3.4.4. Logical Analysis

This module is brain of the entire design. This module evaluates and categorizes traffic depending on standard VoIP behavior and flow pattern. The rules for this module can be modified according to pattern and behavior of type of data and the statistical analysis. Decision making and classification of the traffic can be done according to the historical rules of plain VoIP and known grey traffic. Different criterion metrics can be considered for subsequent classification. Analysis parameters and their weights are discussed in the following section.

3.5. Analysis Parameters

To define the rules being followed by the grey VoIP traffic, we studied the behavior of the standard VoIP traffic at an Internet service provider (ISP). We also generated different types of traffic at the laboratory, as under:

- Plain VoIP traffic.
- Network layer encrypted VoIP traffic.
- Transport layer encrypted VoIP traffic.
- Application layer encrypted VoIP traffic.
- Distributed VoIP traffic.
- Encrypted non VoIP traffic.

Considering the forensics evidences collection using neural approach providing more efficient results [25], the behavior of different metrics was observed over the test traffic. In order to define the statistical model, six metrics that distinguished VoIP from other traffic flows were considered. According to the observed behavior, different logical weights were assigned to each metric. Accordingly, the observed behavior was modeled for the subsequent pattern and signature matching against the de-shaped VoIP flow. The weighted model was later used for testing and analyses of the de-shaped VoIP traffic. At the end, acquired results were compared against the plain VoIP flow. The different metrics and their significance for the commercial grey VoIP were computed as under:

3.5.1. 24 Hour Traffic Flow

Most significantly, we observed that each telecommunication operator runs its operations around the clock. Although traffic intensity varies with different hours of the day, but, global time zone variations provide international telecommunication operations for the 24 hours of the day. This condition was the first to check to ascertain if the traffic between any IP pair flow operates round the clock with negligible null periods or not. The null activity periods between different sessions of a same IP pair occurring at same time can highlight distributed traffic paths. After analysis of different network traffic flows and considering the practical outage periods, the threshold for this criterion was observed to a minimum of 22 hours in a day for any commercial VoIP traffic flow.

3.5.2. Multiple Simultaneous Sessions

Usage statistics of the Internet [24] showed that ISPs providing VoIP connections had very high probability of maintaining multiple sessions simultaneously, than non VoIP traffic. This metric provides a base line to distinguish a commercial telecommunication operator from a non-commercial telecommunication usage, such as voice chat. The commercial VoIP flow between two international telecommunication operators will not be restricted to a single user at a time as in case of peer to peer VoIP flows (Skype). Hence, each commercial VoIP flow contains traffic of multiple simultaneous users. In case, if the network layer encryption is used, session information may not accessible even with the deep packet analyses. This limitation may always be observed for the grey VoIP traffic, due to involvement of the encryption.

3.5.3. Continuous Traffic Flow

As large number of customers' uses telecommunication services globally, the probability for the null periods in a VoIP flow, between two VoIP gateways, remain extremely low. Contrary to the VoIP flow for the telecommunication operator, other encrypted flows are either time restricted (e.g. working timings) or activity restricted (e.g. day, night or late night hours). From a standard commercial VoIP flow, we observed three different time brackets providing intensive VoIP usage. These flows were also compared against the call flow behavior curves of different telecommunication operators. However, these timings may vary basing on the national culture and the climatic conditions. The intensive VoIP usage was observed during:

- Morning 0900 to 1100 hours.
- Afternoon 1500 to 1700 hours.
- Evening 1900 to 2100 hours.

The first two time brackets clearly link the activity within the office hours. However, the evening time bracket provides a useful baseline segregating office activities from the non-office activities.

This condition can be checked if the traffic flow between any specific IP pair remains continuous between any specific start and end timings. For the continuous flow, we observed that the payload during entire session remain non zero for any specific IP pair. As all VoIP codec continuously generate some network traffic even in the absence of the voice activity, repeated nulls during continuous sessions can lead to non VoIP traffic. This condition, coupled with the fact that multiple VoIP sessions have a very low probability of being on hold at the precise same moment, is a very unlikely scenario in a commercial VoIP connection. The threshold for this condition was observed to 2.5 minutes at a stretch.

3.5.4. Bi-Directional Flow

The normal data flow for Internet usage (less VoIP) was generally observed as asynchronous. However, the commercial telecommunication based VoIP flows are generally bidirectional and highly synchronous involving chat from both ends. The bidirectional flow of the traffic is an integral feature of any commercial VoIP traffic. The ratio between sent and received data for the telecommunication based VoIP flows were computed close to the unity. The same ratio for the browsing, data downloading, gaming or unidirectional media streaming remained highly fractional.

This emphasizes on the fact that in the VoIP connection, the traffic load in both directions is almost equal. After observing different realistic flows, the threshold for this condition was set to 60-40, i.e. approximately no side of the end VoIP gateways generate more than 60% of the total data. This can also be stated as each party during a commercial VoIP activity must contribute at least 40% of the total data transferred.

3.5.5. Packet Arrival Time Distribution

Researchers [26] have computed voice activity detection using the packet energy in time domain as well as frequency domain. In case of the telecommunication based bidirectional VoIP flow, the packet arrival rate follows Gaussian distribution around some mean value of jitter [6,26] The jitter value depends on buffer space, processing and transmission delay. The quality of service requirement for the commercial VoIP is highly sensitive to jitter and delay. Disregard of the codec used, a VoIP behavior remains continuous in nature [26], even in the absence of any user activity. This specific phenomenon creates continuous network traffic even in the absence of voice activity for VoIP. On contrary, other non VoIP applications generally link network traffic with user activity only, e.g. financial transactions, etc.

3.5.6. Relation between Packet Size and Packet Arrival Time Distribution

A VoIP traffic mixed with the non VoIP traffic may generate variable sized packets over the network. As segregation of the encrypted VoIP from the normal Internet data flow, without deep packet analyses is a tricky task. However, if ingress and egress data can be segregated in relation to their packet size, graph of arrival time distribution can provide the enhanced view of the flow behavior [6,26]. Effect of the different codec on the packet arrival time against the packet size is a significant intelligence for classification of VoIP [6].

3.6. Logical Decision Rules

The efficiency of our entire model depends upon the logical decision rules applied over the captured network data. The logical model was intended to be generic, to cater all kind of the hybrid mechanisms. After the detailed analysis of the plain VoIP, lab generated grey VoIP and non VoIP traffic; different metrics were computed for their mathematical weights. The weights were computed through evaluation of known VoIP traffic. The computed weights were assigned to the end curves according to its importance in the detection of VoIP traffic. Accordingly, the encrypted network traffic in the different suspicious levels is classified. The bi-directional flow of traffic was considered as the most important criterion, owing to peculiar characteristic of VoIP traffic.

Besides assigning specific weight to the different criterion, additional weights were computed to the combination of criterion. This proved to be helpful in the scenarios where multiple criterion of different importance is met. For the initial assessment, we considered first four metrics, i.e. bi-directional traffic flow, 24 hour flow, continuity of traffic and multiple sessions. Subsequently, all possible combinations were computed for the weight assignment against first four metrics. Each metric was optimized independently by keeping all other metrics as constant. We assigned weights out of total score of 100, out of which 75% weight was marked to individual metrics and remaining 25% to the combination of metrics.

3.6.1. Individual Weights

Assignment of weight to the selected metric is a tricky task, as the situation may vary from one network to other and from one country to other. Moreover such assignment requires regular update according to network statistics.

Determination of weight was a tricky task and required detailed and lengthy traffic analysis. For the purpose of weight assignment, we captured raw internet traffic and observed following:

- As a fraction of overall traffic, UDP packets were observed as 5%-15% of total, and 15%-25% of total flows.
- Determined TCP flows were approximately 4.8 times more than UDP flows.
- Traffic share of VoIP was approximately 0.9%, out of total internet share.
- VoIP showed a gradual increase in volume over the course of the day, well into 19:00 hours before tailing off more abruptly into midnight.
- VoIP traffic rise in the late evening and early morning hours as a proportion of overall traffic.
- Most of the IP layer encrypted sessions frequently last more than 1 hour in duration.
- Although IP layer encrypted sessions count remained negligible. However, such sessions contained 5% of total data.
- DNS traffic share is negligible among overall network traffic.

To acquire these weights, two public sector ISPs were analyzed for the real traffic. According to [3], both ISPs consume 75% of the Internet bandwidth in Pakistan. After acquisition of the statistics for entire week, the traffic evaluation was carried out for the known VoIP traffic. Initially, each factor was assigned individual weight as under:

- Bi-Directional Traffic Flow. This metric was observed as of prime importance due to peculiar commercial VoIP traffic flow behavior.

  This statistics provided baseline for subsequent weight assignment. Considering the encrypted tunnels, we further short listed VoIP and IP layer encrypted flows for assessment of weight for bidirectional traffic. These two type of traffic shares approximately 6% of total data only. Resultantly, determination of bi-directional traffic could easily lead to bi-directional VoIP traffic.

  For fair weight distribution, we limit a single weight to maximum of 50%. According to the traffic analysis, bi-directional traffic is used for bi-directional audio and video flows only. Considering these two types of traffics and according to result over multiple test flows, we found 25% weight for the metric as an optimum value.
- Twenty Four Hour Flow. Due to the commercial business nature of the grey traffic, this metric was observed as second critical in the list. We computed 20% weight for the metric as an optimum value.
- Continuous Traffic Flow. Subject to the smoothness of the VoIP flow and the actual existence of multiple sessions (even if hidden due to the encryption), we considered this metric as third in priority. We observed the weight of 15% to the metric as an optimum value.
- Multiple Sessions. We observed that multiple session information is another basic characteristic of commercial VoIP. However, due to presence of encryption, this metric computation might not be possible. Resultantly we found this metric as fourth in

the priority list. We computed weight of 15% to the metric as an optimum value.

3.6.2. Weights for Combination of Criteria

The combination weight of different metrics was a critical evaluation of the model. After evaluating multiple flows of test data, we considered following %age weights to different combinations as an optimum value:

- Bi-directional + Continuous + 24Hour + Multiple Session = 25%
- Bi-directional + 24Hour + Multiple Session = 23%
- Bi-directional + Continuous + 24Hour = 23%
- Bidirectional + Continuous + Multiple Session = 13%
- Bi-directional + 24Hour = 18%
- Bidirectional + Multiple Session = 8%

3.6.3. Categorization of Flow

After assignment of different weights to the individual and combination of metrics, threshold values were computed for assessment categorization as under:

- According to the behavior of different test cases, any flow with total weight score greater than 75% was observed as logically confirmed VoIP traffic. Hence such unknown traffic could be assumed as "Grey" with high probability.
- Due to presence of encryption and distributed & hidden flows, the traffic with weight greater than 50% value was observed as logically confirmed VoIP traffic with anomalies. Such traffic is categorized as "Suspicious".
- The traffic with less than 50% weight was observed as logically confirmed non VoIP traffic and same is categorized as "Non- suspicious".

4. Testing & Evaluation

After development of a comprehensive detection model, we tested it through a test bed to detect the IP's involved in encrypted VoIP traffic. We developed the test in C++ under Linux environment. The test bed was developed to handle multiple protocols. These protocols include network, transport and application layer protocols, with and without encryption. We performed traffic analysis on IP, IPSec in both AH and ESP mode and PPTP from network layer. TCP, UDP, TLS and SSL from transport layer and SSH and other proprietary protocols from the application layer were also tested. The test bed was divided into four different independent modules as described above. Functionality and run time behavior of the each module was tested independently to ensure its functionality and behavior according to load requirements and accuracy.

Multiple tests were performed over 2 Mbps link of laboratory generated data flow. Initially different data flows up to 2 Mbps throughput were generated at lab and testing was conducted for different modules. After successful lab testing, real flow testing for real traffic was conducted at core ingress router of both the ISPs involved in termination of international VoIP traffic. Multiple test cases were evaluated during the process for week long duration as under:

- Initially, we tested capture mode on 2 Mbps of laboratory generated traffic as test case-1. The test included plain VoIP and encrypted VoIP and non VoIP traffic.
- Later as test case-2, we verified capture mode by mirroring Internet traffic from a mirrored link on the main ingress router of the Internet service providers.
- In test case-3, we tested performance and reliability of the Processed Packet Library using data of test case-1.
- In test case-4, the Processed Session Library was thoroughly tested by using output of the test case-2.
- In test case-5, we tested Analysis module with the output data of test case-3. Subsequently we verified the results of test case-4 by matching it accordingly.

Module-1 (capture mode) was observed as successful in capturing the packets without disturbing the overall network traffic. We also verified the results with the open source Wireshark tool for correctness.

Module-2 (header reconstruction) was observed as resource hungry. However, non linkage of this module with the online routers, allowed parallel processing on multiple machines.

Module-3 (flow reconstruction) was also successful in its performance on both types of traffic.

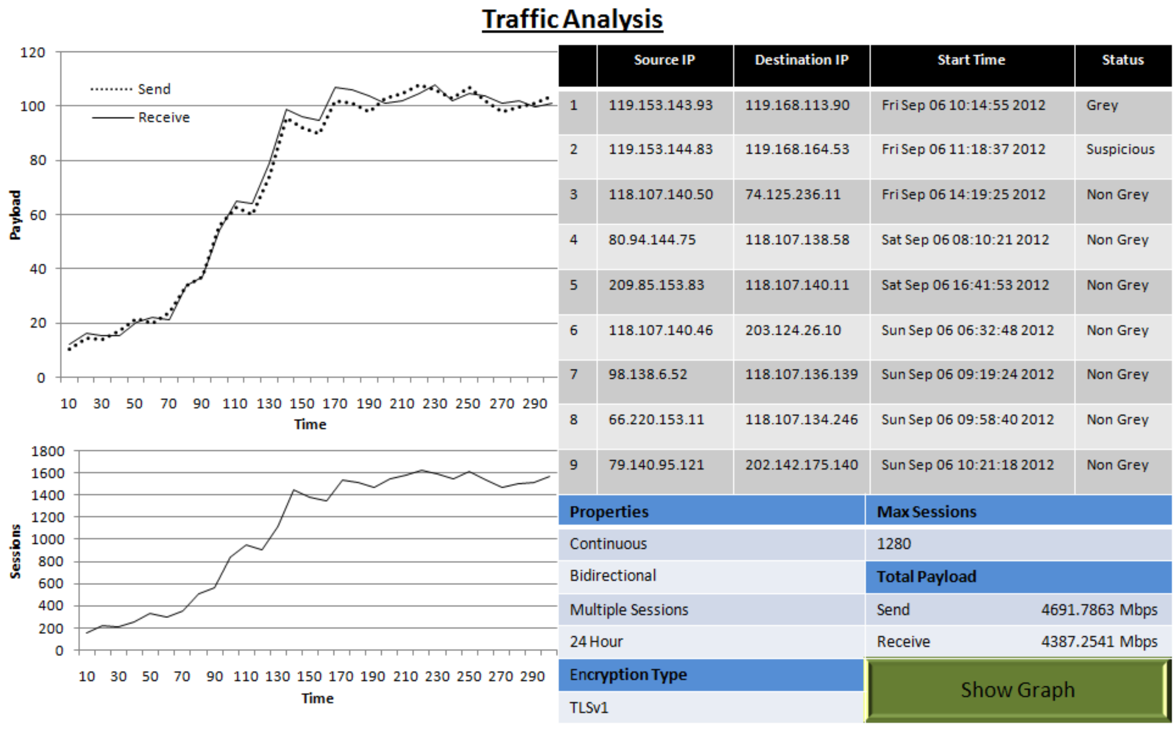
Output of the Module-4 (flow categorization) initially generated few false results due to mismatching of the weight assignment. However, after adjustment of weights for optimum values according to test data, efficiency improved to greater than 90% correct assessment. Different nature of results was also observed with different levels of the suspicion.

Figure 6 shows the output presentation for the module-4. The top right portion shows the runtime state of the filtered IP addresses, along with the start time and the current status. The lower right portion shows the details of the selected IP pair. This portion presents behavior of the flow, type of encryption, total sent and received data and maximum number of the sessions recorded. Top right portion shows the payload graph of the sent and received data for the selected IP pair. The x-axis shows the time elapsed, whereas y-axis shows the payload in Mbps. Lower right portion shows the session graph of the selected IP pair. The x-axis shows the time elapsed, whereas y-axis shows the number of recorded and decrypted sessions.

Subsequently, 24 hour traffic was captured and processed. Accordingly, the graphs for behavior were drawn. Figure 7 shows results for the non-suspicious traffic that does not fulfill the modeled conditions. The left portion shows the payload graph of the sent and received data for the selected IP pair. The x-axis shows the time elapsed, whereas y-axis shows the payload in Mbps. The right portion shows the session graph of the selected IP pair. The x-axis shows the time elapsed, whereas y-axis shows the number of the recorded and decrypted sessions. As sent and received ratio of the flow is greater than 60-40, so the traffic failed to satisfy bidirectional condition. Similarly, it can be seen that available session information shows session count up to six.

Figure 8 shows the behavior for a moderate suspicious traffic. The left portion shows the payload graph of the sent and received data for the selected IP pair. The x-axis shows the time elapsed, whereas y-axis shows the payload in Mbps. The right portion shows the session graph of the selected IP pair. The x-axis shows the time elapsed, whereas y-axis shows the number of the recorded and decrypted sessions. It is clear that both sent and received traffic is almost equal or below 60-40 ratio, depicting the bidirectional behavior. However the session information is not visible because of the IPSec encryption. As the multiple session condition is not satisfied, therefore this type of behavior is categorized as “moderate suspicious”.

Figure 9 shows the behavior of grey traffic that fulfills all four conditions. The left portion shows the payload graph of the sent and received data for the selected IP pair. The x-axis shows the time elapsed, whereas y-axis shows the payload in Mbps. The right portion shows the session graph of the selected IP pair. The x-axis shows the time elapsed, whereas y-axis shows the number of recorded and decrypted sessions. It can be clearly seen that session number ranges from 35 to 60 or more. Hence, multiple session condition is also satisfied.



	Source IP	Destination IP	Start Time	Status
1	119.153.143.93	119.168.113.90	Fri Sep 06 10:14:55 2012	Grey
2	119.153.144.83	119.168.164.53	Fri Sep 06 11:18:37 2012	Suspicious
3	118.107.140.50	74.125.236.11	Fri Sep 06 14:19:25 2012	Non Grey
4	80.94.144.75	118.107.138.58	Sat Sep 06 08:10:21 2012	Non Grey
5	209.85.153.83	118.107.140.11	Sat Sep 06 16:41:53 2012	Non Grey
6	118.107.140.46	203.124.26.10	Sun Sep 06 06:32:48 2012	Non Grey
7	98.138.6.52	118.107.136.139	Sun Sep 06 09:19:24 2012	Non Grey
8	66.220.153.11	118.107.134.246	Sun Sep 06 09:58:40 2012	Non Grey
9	79.140.95.121	202.142.175.140	Sun Sep 06 10:21:18 2012	Non Grey

Properties	Max Sessions	
Continuous	1280	
Bidirectional	Total Payload	
Multiple Sessions	Send	4691.7863 Mbps
24 Hour	Receive	4387.2541 Mbps
Encryption Type	Show Graph	
TLSv1		

Figure 6. Output for Module-4

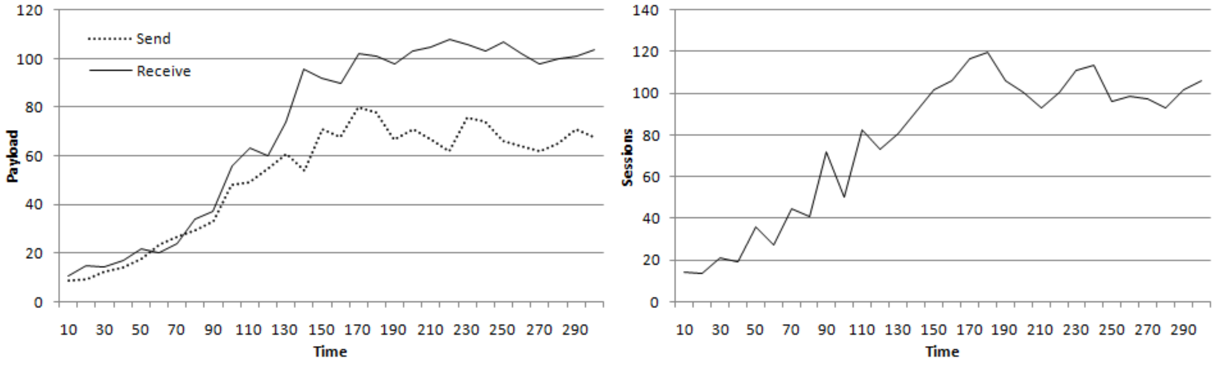


Figure 7. Graph for the Data Flow and Session against Time Showing Behavior of the Non-suspicious Traffic

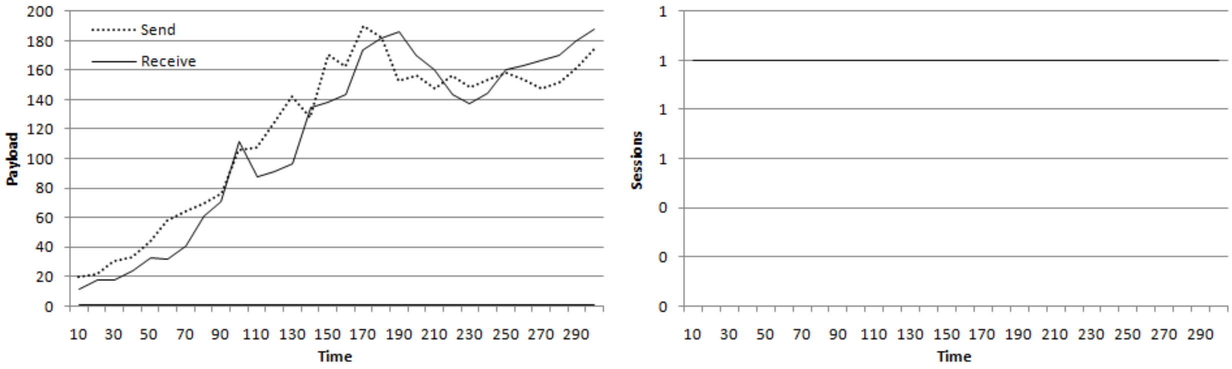


Figure 8. Graph for the Payload and Session against Time Showing Behavior of Moderate Suspicious Traffic

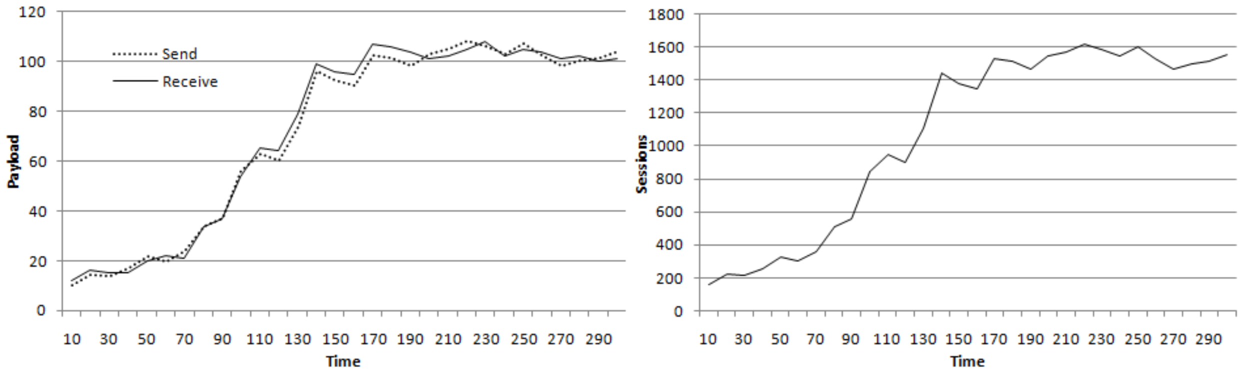


Figure 9. Graph for the Payload and Sessions against Time Showing Behavior of Grey Traffic

5. Conclusion

The growth of illegal VoIP activity is a lucrative platform for culprits to earn huge revenue and causes huge financial losses to the state. VoIP intrusion detection against commercial traffic is a tricky affair as many domestic Internet users legally employ VoIP for the point-to-point direct communication. It requires thorough statistical and behavioral analysis over a period of time to identify and detect IP addresses involved in this crime. Subsequently, one can segregate illegal IPs form the network traffic. In addition, involvement of the encryption techniques and availability of the high throughput Internet connections at cheap rates, has made the problem complicated many folds.

In this proposed technique, instead of encryption analysis, we have endeavored to deploy VoIP based Intrusion Detection System using the statistical flow analysis coupled with the behavior analysis. It deals with the profile development and anomaly detection based on the variation from this profile of VoIP traffic based on observed patterns. The encryption is detected and the layer on which encryption is done is found. The encryption layer information helps to identify the type of the encryption technique used. It can prove to be helpful in computing the statistical parameters for the better decision making.

The end results show significant success on the proposed approach towards the solution of the problem.

References

[1] Nabil Schear and Nikita Borisov “Preventing SSL Traffic Analysis with Realistic Cover Traffic (extended abstract)” 16th ACM Conference on Computer and Communications Security, CCS 2009.

[2] Sen. Patrick Leahy “Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act of 2011”, 112th US Congress, 2011-2012.

[3] PTA, “PTA ANNUAL REPORT 2008-09-10” Annual Reports Published by Pakistan Telecommunication Authority, online available on http://www.pta.gov.pk/annual-reports, 2010.

[4] ITU “The Status of Voice over Internet Protocol (VoIP) Worldwide, 2006” Report published by International Telecommunication Union, The Future of Voice Document, January 2007.

[5] Choudhary, M.A.; Aftab, H “Optimizing financial parameters to disincentives international grey traffic and rationalization of measures to curb illegal international telephony in Pakistan” IEEE International Technology Management Conference (ITMC), 2011.

[6] Toshiya Okabe, Tsutomu Kitamura, and Takayuki Shizuno. “Statistical traffic identification method based on flow-level behavior for fair VoIP service” 1st IEEE workshop on VoIP Management and Security (VoIP MaSe), April 2006.

[7] Riyad Alshammari and A. Nur Zincir-Heywood “Unveiling Skype Encrypted Tunnels using GP” IEEE Congress on Evolutionary Computation (CEC), 2010.

[8] Stephens, A., and P. J. Cordell. "SIP and H. 323—interworking VoIP networks." BT technology journal 19.2 (2001): 119-127.

[9] JPG Dalton Jr, SA Thomas “Clearinghouse server for Internet telephony and multimedia communications” US Patent 7,017,050, 2006.

[10] Angelos D. Keromytis, “Survey of VoIP Security Research Literature” Voice over IP Security, Springer Briefs in Computer Science, 1, 27-55, 2011.

[11] Carlos Scott and Chez Ciechanowicz, “Covert channels of communication hidden inside legitimate networks cannot be eliminated but they can be significantly reduced by careful design and analysis”, Information Security Group at Royal Holloway, University of London, 2008.

[12] Thomas Porter, C. I. S. S. P., and CCDA CCNP. Practical VoIP Security. Syngress, 2006.

[13] Chou, W. “Strategies to Keep Your VoIP Network Secure” IEEE IT Professional September.-October. 2007.

[14] Robert Birke, Marco Mellia, Michele Petracca, Dario Rossi “Experiences of VoIP traffic monitoring in a commercial ISP” International Journal of Network Management Special Issue: Traffic Monitoring and Network Measurements: from Theory to Practice, 20(5), 339-359, September/October 2010.

[15] M. Dusi, M. Crotti, F. Gringoli and L. Salgarelli “Tunnel Hunter: Detecting Application-Layer Tunnels with Statistical Fingerprinting”, Elsevier, Journal of Computer Networks, 53, 81-97, 2009.

[16] Taner Yildirim and Dr. PJ Radcliffe “VoIP Traffic Classification in IPSec Tunnels”, International Conference on Electronics and Information Engineering (ICEIE 2010).

[17] A. W. Moore and D. Zuev “Internet traffic classification using Bayesian analysis techniques”, In SIGMETRICS ’05: Proceedings of the 2005 ACM SIGMETRICS international conference on Measurement and modeling of computer systems, pages 50-60, New York, NY, USA, 2005. ACM Press.

[18] N. Williams, S. Zander, and G. Armitage “A preliminary performance comparison of five machine learning algorithms for practical IP traffic flow classification” SIGCOMM Computer. Communication. Rev., 36(5):5-16, 2006.

[19] E. Alpaydin “Introduction to Machine Learning” MIT Press, 2004.

[20] J. Doucette and M. Heywood “Gp Classification under Imbalanced Data Sets: Active Sub-sampling and AUC Approximation”, In European Conference on Genetic Programming, volume. 4971 of Lecture Notes in Computer Science, pages 266-277, 2008.

[21] Chappell, Laura A. Wireshark Network Analysis: The Official Wireshark Certified Network Analyst Study Guide. Protocol Analysis Institute, Chappell University, 2010.

[22] Caswell, Brian, Jay Beale, and Andrew Baker. Snort Intrusion Detection and Prevention Toolkit. Syngress, 2007.

[23] Snex A/S “Application Visibility and Risk Report”, A report on Network Traffic by Paloalto Networks, April 19, 2011.

[24] Bing Li, Zhigang Jin , Maode Ma, ”VoIP Traffic Identification Based on Host and Flow Behavior Analysis”, 6th International

Conference on Wireless Communications Networking and Mobile Computing (WiCOM), 2010.

[25] Pelaez, J.C.; Fernandez, E.B, “VoIP Network Forensic Patterns” Fourth International Multi-Conference on Computing in the Global Information Technology, 2009. ICCGI '09.

[26] Venkatesha Prasad, R., et al. "Comparison of voice activity detection algorithms for VoIP." Computers and Communications, 2002. Proceedings. ISCC 2002. Seventh International Symposium on. IEEE, 2002.