International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 3 Issue: 2 482 - 488

An Overview of Network Traffic Classification Methods

Ms. Zeba Atique Shaikh
M.E. (Computer Science & Engg. Student)
Prof. Ram Meghe College of Engineering & Management, Badnera, Amravati
zeba.shaikh2207@gmail.com

Prof. Dr. D.G. Harkut,
Associate Professor (Computer Science & Engg.)
Prof. Ram Meghe College of Engineering & Management, Badnera, Amravati
d.harkut@rediffmail.com

***Abstract*—** Network traffic classification can be used to identify different applications and protocols that exist in a network. Actions such as monitoring, discovery, control and optimization can be performed by using classified network traffic. The overall goal of network traffic classification is improving the network performance. Once the packets are classified as belonging to a particular application, they are marked. These markings or flags help the router determine appropriate service policies to be applied for those flows. This paper gives an overview of available network classification methods and techniques. Researchers can utilize this paper for approaching real time network traffic classification. Traffic classification using payload, statistical analysis, deep packet inspection, naïve Bayesian estimator and Bayesian neural networks are reviewed in this paper.

Keywords- *network traffic classification; payload; statistical analysis; deep packet inspection; neural networks; statistical fingerprinting; traffic classes*

*****

I. INTRODUCTION

Traffic classification is an automated process which categorizes computer network traffic according to various parameters (for example, based on port number or protocol) into a number of *traffic classes* [1]. Each resulting traffic class can be treated differently to differentiate the service implied for the user (data generator/ consumer). Packets are classified to be differently processed by the network scheduler. Upon classifying a traffic flow using a particular protocol, a predetermined policy can be **applied** to it and other flows to either guarantee a certain quality (as with VoIP or media streaming service) or to provide best-effort delivery. This may be applied at the ingress point (the point at which traffic enters the network) with a granularity that allows traffic management mechanisms to separate traffic into individual flows and queue, and shape them differently. Classification is achieved by various means.

First approach is by using port numbers. This method is fast and low resource-consuming. It is supported by many network devices. It does not implement the application-layer payload, so it does not compromise the users' privacy. It is useful only for the applications and services, which use fixed port numbers hence easy to cheat by changing the port number in the system. Second approach is by using Deep Packet Inspection which inspects the actual payload of the packet. It detects the applications and services regardless of the port number, on which they operate. Lack support for many applications, as Skype, which is badly supported by most classifiers. It is slow, requires a lot of processing power, signatures must be kept up to date, as the applications change very frequently and due to encryption, makes in many cases this method impossible. Matching bit patterns of data to those of known protocols is a simple, yet widely used technique. An example to match the BitTorrent protocol handshaking phase would be a check to see if a packet began with character 19 which was then followed by the 19-byte string 'BitTorrent protocol'. A comprehensive comparison of various network traffic classifiers, which depend on Deep Packet Inspection (PACE, OpenDPI, 4 different configurations of L7-filter, NDPI, Libprotoident, and Cisco NBAR), is shown in the Extended Independent Comparison of Popular Deep Packet Inspection (DPI) Tools for Traffic Classification [2]. Third methodology includes approaches based on statistical classification which relies on statistical analysis of attributes such as byte frequencies, packet sizes and packet inter-arrival times. It often uses Machine Learning Algorithms, as K-Means, Naive Bayes Filter, C4.5, C5.0, J48, or Random Forest. This technique is fast technique compared to port-based classification. It can detect the class of yet unknown applications.

The overall network traffic can be broadly categorized into three types: Sensitive, Best-Effort, and Undesired. Sensitive traffic is traffic the operator has an expectation to deliver on time. This includes VoIP, online gaming, video conferencing, and web browsing. Traffic management schemes are typically tailored in such a way that the quality of service of these selected uses is guaranteed, or at least prioritized over other classes of traffic. This can be accomplished by the absence of shaping for this traffic class, or by prioritizing sensitive traffic above other classes. Best effort traffic is all other kinds of non-detrimental traffic. This is traffic that the ISP deems isn't

sensitive to Quality of Service metrics (jitter, packet loss, latency). A typical example would be peer-to-peer and email applications. Traffic management schemes are generally tailored so best-effort traffic gets what is left after sensitive traffic. Undesired traffic category is generally limited to the delivery of spam and traffic created by worms, botnets, and other malicious attacks. In some networks, this definition can include such traffic as non-local VoIP (for example, Skype) or video streaming services behaviour-based BLINC method and seven common to protect the market for the 'in-house' services of the same statistical feature based methods using supervised type. In these cases, traffic classification mechanisms algorithms on seven different traffic traces. identify this traffic, allowing the network operator to either Traffic classification technique plays an important role in block this traffic entirely, or severely hamper its operation. modern network security and management architectures [4], II. RELATED WORK [5]. For instance, traffic classification is normally an essential component in the products for QoS control [6] and The goal of network traffic classification is to classify intrusion detection [7], [8]. With the popularity of cloud traffic flows according to their generation applications. The computing [9], the amount of applications deployed on the current research of traffic classification concentrates on the Internet is quickly increasing and many applications adopt application of machine learning techniques into flow the encryption techniques. This situation makes it harder to statistical feature based classification methods [4]. The flow classify traffic flows according to their generation statistical feature based traffic classification can avoid the applications. Traditional traffic classification techniques rely problems suffered by previous approaches such as dynamic on checking the specific port numbers used by different ports, encrypted applications and user privacy protection. applications, or inspecting the applications' signature strings Many supervised classification algorithms have been in the payload of IP packets [11]. These techniques applied to traffic classification by taking into account encounter a number of problems in the modern network such various network applications and situations. In early works, as dynamic port numbers, data encryption and user privacy Moore and Zuev [12] applied the naive Bayes techniques to protection. Currently, the state of-the-art methods tend to classify network traffic based on the flow statistical features. conduct classification by analyzing flow level statistical Later, several well-known algorithms were also applied to properties [3], [12]. Substantial attention has been paid on traffic classification, such as Bayesian neural networks [14] the application of machine learning techniques to flow and support vector machines [15]. Erman et al. [1] proposed statistical features based traffic classification [4]. However, to use unidirectional statistical features to facilitate traffic the performance of the existing flow statistical feature based classification in the network core. For real-time traffic traffic classification is still unsatisfied in real world classification, several supervised classification methods [13] environments. A number of supervised classification were proposed, which only use the first few packets. Other algorithms and unsupervised clustering algorithms have been existing works include the Pearson's chi-Square test based applied to network traffic classification. In supervised traffic technique [1], probability density function (PDF) based classification [12], [6], [13], [15], the flow classification protocol fingerprints, and small time-windows based packet model is learned from the labeled training samples of each count [12]. The supervised traffic classification approach predefined traffic class. The supervised methods classify any can achieve high classification performance for known flows into predefined traffic classes, so they cannot deal with applications when there is sufficient pre-labeled data, while unknown flows generated by unknown applications. it cannot handle unknown applications. Moreover, to achieve high classification accuracy, the By contrast, the clustering-based approach has the supervised methods need sufficient labeled training data. By potential to deal with unknown applications. It applies the contrast, the clustering-based methods can automatically unsupervised clustering algorithms to categorize a set of group a set of unlabelled training samples and apply the unlabelled training samples and uses the produced clusters clustering results to construct a traffic classifier. In these to construct a traffic classifier. McGregor et al. [16] methods, however, the number of clusters have to be set proposed to group traffic flows into a small number of large enough to obtain high-purity traffic clusters. It is a clusters using the expectation maximization (EM) algorithm difficult problem of mapping from a large number of traffic and manually label each cluster to an application. Some clusters to a small number of real applications without other well-known clustering algorithms such as AutoClass, supervised information. k-means and DBSCAN were also applied to traffic III. TRAFFIC CLASSIFICATION classification. Bernaille et al. [17] applied the k-means algorithm to traffic clustering and labeled the clusters to Network traffic classification can be categorized into: applications by using a payload analysis tool. pay-load based traffic classification and statistical analysis Some empirical study evaluated the traffic classification based traffic classification. In Payload-Based Classification performance of different methods for practical usage. method, packets are classified based on the fields of the Roughan et al. [6] have tested NN and LDA methods for payload, such as Layer 4 ports (source or destination or traffic classification using five categories of statistical both). Statistical method uses statistical analysis of the features. Williams et al. [1] compared the supervised traffic behavior like inter-packet arrival, session time, and algorithms including naïve Bayes with discretization, naive so on. The payload-based method is most prevalent. Bayes with kernel density estimation, C4.5 decision tree, However, more often than not, it fails with encrypted and Bayesian network and naïve Bayes tree. Kim et al. [13] tunneled traffic. The Payload-Based Classification extensively evaluated ports-based CorelReef method, host

 ISSN: 2321-8169
482 - 488

technique can be divided into generic or basic payload analysis or advanced payload analysis. The generic approach to traffic classification is based on the IP header. Typically, the information looked at is: Layer 3 address (IP address), Layer 2 address (MAC) and Protocols. This technique is very simple and does not provide proper classification. A classification method based on the assignment of traffic is not widely used.

All generic classification techniques based on Destination IP address, Source IP address, or IP protocol, etc. are limited in their ability as the inspection is limited to the IP header only. Similarly, classifying based on Layer 4 ports only is also limited. The problem with this approach is that not all current applications use standard ports. Some applications even obfuscate themselves by using well the defined ports of other applications (e.g., IM applications may run over TCP port 80, which is generally used for HTTP). Hence, the Layer 4 port mechanism of application identification is not always reliable. Advanced classification techniques rely on deep packet inspection (DPI). There are varieties of DPI techniques, such as pattern analysis or behavior analysis. These are much more reliable than the generic classification technique. The following figure 1 illustrates various classification methods and techniques.

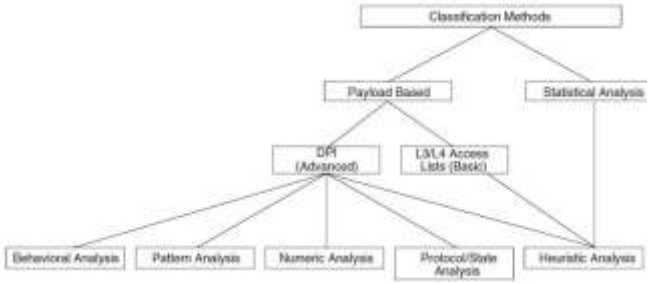

Figure 1: Network Traffic Classification Methods and Techniques.

A. Payload-Based Traffic Classificaation

Payload-based classification methods can also be divided based on the processing method used for classifying traffic. There are four methods, all of them use one or more payload inspection techniques like Deep Packet Inspection to verify and classify traffic. Packet-Based No State (PBNS) is the simplest and involves checking the payload for certain parameters like port numbers. It is less taxing on the CPU. For example, a simple access-list based port matching like the one below can identify all Telnet traffic.

access-list 101 permit tcp any any eq telnet

This method typically utilizes the basic payload-based classification technique. However, as already discussed, it is not always accurate or fully usable as the classification is on a per-packet basis without regard to an application session and is also limited by how deep inside the packet the verification of the flow goes.

Packet-Based per Flow State (PBFS) method is based on flows. A flow is defined as a sequence of packets from a sending application to a receiving application. In this method, a table to track each session based on the 5 tuples (source address, destination address, source port, destination port, and the transport protocol) is maintained for each flow. Since a flow has multiple packets, once a packet is marked as belonging to an application all subsequent packets in the flow need to be marked as such. For example, in a typical VoIP call, H.323 is used for setting up the call and then RTP/RTCP is used for carrying the actual voice traffic. Once a H.323 flow is identified and marked, subsequent RTP/RTCP flows to the same source IP/destination IP pair are tagged with the same parameters.

Message-Based per Flow State (MBFS) method is similar to PBFS, except that this operates on messages instead of packets. A message is protocol dependent and is an information element that can span multiple packets or a single packet can contain multiple messages. Since it operates on messages there needs to be some sort of TCP normalizer to take care of IP fragments and TCP Segments. Since entire messages have to be considered, there is a considerable increase in memory requirements. In the Message-Based per Protocol State (MBPS) method, not only is the application tracked but also what the application is transmitting. In other words, complete knowledge of the protocol state machine is needed to implement this method. This is the most taxing method on the CPU and has more memory requirements too. The last three methods, PBFS, MBFS, and MBPS, utilize advanced classification techniques that are based on DPI.

B. Deep Packet Inspection

Although most general applications can be determined or at least guessed based on L3 and L4 information, additional granular sub-classes within applications (like URLs) or specific kinds of messages within the application (like voice within IM streams) are required. For proper classification and sub-classification, it is necessary to do a deep packet inspection (DPI) and verify what the application is. Most DPI mechanisms use Signature Analysis to understand and verify different applications. Signatures are unique patterns that are associated with every application. In other words, each application is studied for its unique characteristics and a reference database is created. The classification engine then compares the traffic against this reference to identify the exact applications. That means the reference needs to be updated periodically to keep current with new applications as well as new developments in existing protocols. There are different Signature Analysis methods. The most popular methods include: Pattern analysis, Numerical analysis, Behavioral analysis, Heuristic analysis and Protocol/state analysis.

Some applications embed certain patterns (bytes/characters/string) in the payload of the packets, which can be used by the classification engine to identify such protocols. Depending on the application, these patterns may not necessarily be always located at a specific deterministic offset. The patterns might be present in any position in the

packet. Still, the classification engine can identify these packets. However, not all protocols embed special pattern, string, or characters in the packets and hence pattern analysis approach will not work for them. Numerical Analysis involves looking into the numerical characteristics of packets such as payload size, number of response packets, and offsets. Older Skype versions (pre-2.0) are good cases for such analysis. The request from client is an 18-byte message and the response it receives is usually 11 bytes. As the analysis may be spread over multiples packets, the classification decision might take more time. Occasionally, analyzing the traffic behavior would produce greater insight into the applications that may be running. This behavior can be used to classify such applications. Similarly, by doing a statistical (heuristic) analysis of the inspected packets, the underlying protocol can be classified. Behavior and Heuristic analysis typically go hand in hand and many of the anti viral programs use these techniques to identify viruses and worms. In some applications, the protocol follows a certain sequence of steps or actions. For example, a typical FTP GET request from a client is followed by a valid response from the server. Such protocol conformance can be used to classify such applications. As more applications start encrypting traffic, it becomes a challenge for any classification mechanism to classify the applications accurately. With encryption, all upper layer information becomes invisible to DPI mechanisms. Behavior and heuristic analysis methods can help to identify some applications. Newer classification mechanisms that use behavior and heuristic analysis methods (along with intelligent algorithms, such as clustering algorithms) can help identify encrypted traffic. None of these methods, on their own, can provide satisfactory classification of all applications. Therefore, in a typical deployment these methods are used together.

C. Cisco Classification Technologies

Cisco classification technologies include QoS access lists and DPI engines. Cisco IOS provides the ability to configure Layer 3 or Layer 4 based access lists that can be used with the QoS to classify different types of traffic. Specific QoS classes can be configured to use different access lists to match traffic and based on the match the packets can be marked. The matching can be based on Layer 3 addresses (source/destination IP), Layer 4 protocol or ports, or a combination thereof. In addition to software-based ACLs, Cisco platforms like 6500 & GSR provide the ability to do ACL lookups in hardware. For example in a 6500 platform, these ACLs can be programmed in Ternary Content Addressable Memory (TCAM) and lookups performed against those entries. However, it should be noted that TCAMs have finite memory and without careful planning, the resources can be exhausted. TCAM lookups are much faster than traditional software lookups because they are performed in hardware, so classification based on TCAM lookups is much faster.

DPI engines can be co-resident in the software or can be dedicated hardware. Both have advantages and disadvantages. While a dedicated hardware provides speed and versatility, the cost of deploying such a box restricts their usage to high traffic volume environments like a Data Center or a large Enterprise Branch office. Cisco's Service

Control Engine (SCE) is a good example of a dedicated hardware DPI appliance. Software-based DPI engines are cost effective, but they do consume CPU cycles and hence can be deployed only at low or medium traffic volume environments such as those found in a small or medium Enterprise Branch Office. Cisco Service Control Engine (SCE) is a DPI device that can do DPI and detect traffic patterns at line rates. SCE incorporates many DPI technologies such as protocol/state analysis, pattern analysis, and behavioral and heuristic analysis. SCE can also do subscriber-level classification. The Cisco SCE can be deployed in-band or out-of-band. It is typically deployed in the Data Center. If it is deployed in band, all the traffic in the network passes through SCE. If it is deployed out of band then a copy of all the traffic is passed onto SCE by the DC switch. It should be noted that in out of band mode, the SCE can only perform monitoring.

TABLE I. TRAFFIC CLASSES TO PRIORITY MAPPING

Traffic Type	Traffic Class	Priority
Bulk transfers, Games etc.	Background	1
Less than 10 millisecond delay	Voice	2
Less than 100 millisecond delay	Video	3
Some important application	Controlled Load	4
Best Effort for important users	Excellent Effort	5
Ordinary LAN priority	Best Effort	6
High requirement to get through to maintain and support the network infrastructure	Network Control	7

Network Based Application Recognition (NBAR) is an application-aware classification feature in IOS. NBAR can look deep inside a packet and do stateful analysis of the information in the packet. It can recognize a number of applications, including ones that use ephemeral ports. Even with a given protocol, NBAR can look so deep inside the packets that it can categorize packets that are of the same protocol, but with different protocol-specific parameters. For example, NBAR can classify based on the URL for HTTP packets and based on ICA traffic for CITRIX ICA. Typically, QoS and NBAR are used in conjunction. NBAR is used to recognize specific applications and QoS is used to mark them and provide appropriate treatment based on the markings.

The IEEE 802.1p standard provides traffic class

expediting and dynamic multicast filtering. It enables Layer 2 switches to prioritize traffic. The 802.1p defines 3 bits in the header for classification, which helps classifying traffic into eight different traffic classes. It should be noted that 802.1p is an extension of 802.1Q standard and they work together. IEEE has put forth recommendations on various traffic types, corresponding traffic classes, and priorities to be used with 802.1p standard. They are listed in table 1.

IV. NAÏVE BAYESIAN AND BAYESIAN NEURAL NETWORK BASED TRAFFIC CLASSIFICATION

A traffic classifier that can achieve a high accuracy across a range of application types without any source or destination host-address or port information can be designed using supervised machine learning based on a Bayesian trained neural network. Bayesian neural network (NN) based traffic classifier can produce more accurate results compared to naïve Bayesian traffic classifier. The Bayesian framework using a neural network model allows identification of traffic without using any port or host information. A classification accuracy of over 99% can be achieved when training and testing on homogeneous traffic from the same site on the same day. A classification accuracy of 95% in the (more realistic) situation of training on one day of traffic from one site, and testing on traffic from that site for a day eight months later; this is a figure significantly higher than for the naïve Bayesian approach.

TABLE II. FEATURES DESCRIBING EACH OBJECT THAT CAN BE USED FOR CLASSIFICATION

Features
Flow Metrics (duration, packet-count, total bytes)
Packet inter-arrival time (mean, variance, 1st & 3rd quartiles, median, minimum, maximum)
Size of TCP/IP control fields (mean, variance, 1st & 3rd quartiles, median, minimum, maximum)
Total Packets (in each direction and total for flow)
Payload size (mean, variance, 1st & 3rd quartiles, median, minimum, maximum)
Effective bandwidth based upon entropy
Ranked list of top-ten Fourier-transform components of packet inter-arrival times (for each direction)
Numerous TCP-specific values derived from tcptrace (total payload Bytes, total number of pushed packets, packets, total number of ACK packets, minimum observed segment size)

The features of flows, derived from streams of packet headers have greatest contribution to classifiers based upon a naive Bayesian approach and upon a Bayesian neural network approach. A small number of features carry high significance regardless of the classification scheme. There can be some overlap in features of high importance to either method.

Each object is a flow of data described by its class and a set of features. The original flow data was not available to us, but each object has a number of particular properties, such as the client and server port of each flow, along with a number of characteristics parameterizing its behavior. These features allow for discrimination between the different traffic classes. Table 2 provides a summary of the 246 per-flow features that are available for traffic classification using naïve Bayesian and Bayesian NN approach.

The following table 3 gives the overall comparison of reviewed approaches for network flow classification.

V. CONCLUSION AND FUTURE WORK

Classification involves proper identification of different application flows and packets in the traffic and their appropriate marking. Once the packets are classified, the router can apply appropriate service policies for those packets. Typically, QoS is used to provide appropriate treatment to different traffic based o the configured policies. As was discussed earlier, each application has its own characteristics and requirements. With the limited WAN bandwidth, QoS policies help in providing different treatments for different traffic classes. Various QoS mechanisms such as Congestion Management, Congestion Avoidance, Traffic Policing/Shaping, and Link Efficiency exist that can be used to manage the WAN bandwidth.

A sophisticated Bayesian trained neural network is able to classify flows, based on header-derived statistics and no port or host (IP address) information, with up to 99% accuracy for data trained and tested on the same day, and 95% accuracy for data trained and tested eight months apart.

TABLE III. COMPARATIVE ANALYSIS OF NETWORKCLASSIFICATION METHODS ON THE BASIS OF VARIOUS PARAMETERS

Sr. No.	Paper Title	Methodology Used	Purpose	Datasets Used	Model/Tools/Concept Used	Comparison carried out with	Performance Evaluation Parameters Used
1.	An Effective Network Traffic Classification Method with Unknown Flow Detection [1]	Incorporate flow correlation into semi-supervsied method	Unknown flow detection	Wide and isp http://mawi.wide.ad.jp/mawi/	Nearest cluster based classifier (NCC)	kNN, Naive Bayes, Bayesian Netowrk, and Erman's semi-supervised method	Classification accuracy, Propagation rate, Training purity, False detection rate, True detection rate
		Flow label propagation	Automatically label relevant flows				
		Compound classification	Identify correlated flows				
2.	Extended Independent Comparison of Popular Deep Packet Inspection (DPI) Tools for Traffic Classification [2]	Deep packet inspection	Traffic classification	Generated from file sharing applications, photo-video group, web browsing traffic, Encrypted tunnel traffic, Storage backup traffic, Email management traffic, Games	PACE, OpenDPI, Libprotoident, Cisco Network Based Application Recognition (NBAR), L7-filter	--	Accuracy (In terms of correct, wrong and unclassified %)3.
3.	BLINC: multilevel traffic classification in the dark [3]	Classification at social level	Identify communities of nodes with similar interest	Real time network generated data	Transport layer classification	Payload based classification	Accuracy and Completeness
		Classification at functional level	Identify functional role of host				
		Classification at application level	Identify interaction of host on various ports				
4.	An Effective Network Traffic Classification Method with Unknown Flow Detection [1]	Incorporate flow correlation into semi-supervsied method	Unknown flow detection	Wide and isp http://mawi.wide.ad.jp/mawi/	Nearest cluster based classifier (NCC)	kNN, Naive Bayes, Bayesian Netowrk, and Erman's semi-supervised method	Classification accuracy, Propagation rate, Training purity, False detection rate, True detection rate
		Flow label propagation	Automatically label relevant flows				
		Compound classification	Identify correlated flows				
5.	Extended Independent Comparison of Popular Deep Packet Inspection (DPI) Tools for Traffic Classification [2]	Deep packet inspection	Traffic classification	Generated from file sharing applications, photo-video group, web browsing traffic, Encrypted tunnel traffic, Storage backup traffic, Email management traffic, Games	PACE, OpenDPI, Libprotoident, Cisco Network Based Application Recognition (NBAR), L7-filter	--	Accuracy (In terms of correct, wrong and unclassified %)3.
6.	BLINC: multilevel traffic classification in the dark [3]	Classification at social level	Identify communities of nodes with similar interest	Real time network generated data	Transport layer classification	Payload based classification	Accuracy and Completeness
		Classification at functional level	Identify functional role of host				
		Classification at application level	Identify interaction of host on various ports				

REFERENCES

[1] Jun Zhang, Chao Chen, Yang Xiang, Wanlei Zhou, and Athanasios V. Vasilakos, "An Effective Network Traffic Classification Method with Unknown Flow Detection", *IEEE Transaction on Network and Service Management, Vol 12, Dec 2013*.

[2] Tomasz Bujlow, Valentín Carela-Español, Pere Barlet-Ros. "Extended Independent Comparison of Popular Deep Packet Inspection (DPI) Tools for Traffic Classification". *Universitat Politècnica de Catalunya. Retrieved 2014-02-06*.

[3] T. Karagiannis, K. Papagiannaki, and M. Faloutsos, "BLINC: multilevel traffic classification in the dark," SIGCOMM Comput. Commun. Rev., vol. 35, pp. 229–240, Aug. 2005.

[4] T. T. Nguyen and G. Armitage, "A survey of techniques for internet traffic classification using machine learning," *IEEE Commun. Surveys & Tutorials, vol. 10, no. 4, pp. 56–76, Fourth Quarter 2008.*

[5] A. Finamore, M. Mellia, M. Meo, and D. Rossi, "KISS: stochastic packet

inspection classifier for UDP traffic," *IEEE/ACM Trans. Netw., vol. 18, no. 5, pp. 1505–1515, Oct. 2010.*

[6] M. Roughan, S. Sen, O. Spatscheck, and N. Duffield, "Class-of-service mapping for QoS: a statistical signature-based approach to IP traffic classification," *in Proc. 2004 ACM SIGCOMM Conference on Internet Measurement, pp. 135–148.*

[7] Y. Xiang, W. Zhou, and M. Guo, "Flexible deterministic packet marking: an IP traceback system to find the real source of attacks," *IEEE Trans.Parallel Distrib. Syst., vol. 20, no. 4, pp. 567–580, Apr. 2009.*

[8] Z. M. Fadlullah, T. Taleb, A. V. Vasilakos, M. Guizani, and N. Kato, "DTRAB: combating against attacks on encrypted protocols through traffic-feature analysis," *IEEE/ACM Trans. Netw., vol. 18, no. 4, pp. 1234–1247, Aug. 2010.*

[9] R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg, and I. Brandic, "Cloud computing and emerging it platforms: vision, hype, and reality for delivering computing as the 5th utility," *Future Generation Computer Systems, vol. 25, no. 6, pp. 599–616, June 2009*

[10] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A view of cloud computing," *Commun. ACM, vol. 53, pp. 50–58, Apr. 2010.*

[11] P. Haffner, S. Sen, O. Spatscheck, and D. Wang, "ACAS: automated construction of application signatures," in *Proc. 2005 ACM SIGCOMM Workshop on Mining Network Data., pp. 197–202.*

[12] A. W. Moore and D. Zuev, "Internet traffic classification using Bayesian analysis techniques," *SIGMETRICS Perform. Eval. Rev., vol. 33, pp. 50–60, June 2005.*

[13] H. Kim, K. Claffy, M. Fomenkov, D. Barman, M. Faloutsos, and K. Lee, "Internet traffic classification demystified: myths, caveats, and the best practices," in *Proc. 2008 ACM CoNEXT Conference, pp. 1–12.*

[14] J. Zhang, Y. Xiang, Y. Wang,W. Zhou, Y. Xiang, and Y. Guan, "Network traffic classification using correlation information," *IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 1, pp. 104–117, Jan. 2013.*

[15] A. Este, F. Gringoli, and L. Salgarelli, "Support vector machines for TCP traffic classification," *Computer Networks, vol. 53, no. 14, pp. 2476–2490, Sept. 2009.*

[16] A. McGregor, M. Hall, P. Lorier, and J. Brunskill, "Flow clustering using machine learning techniques," in *Proc. 2004 Passive and Active Measurement Workshop, pp. 205-214.*

[17] L. Bernaille, R. Teixeira, I. Akodkenou, A. Soule, and K. Salamatian, "Traffic classification on the fly," *SIGCOMM Comput. Commun. Rev., vol. 36, pp. 23-26, Apr. 2006*

[18] .G. Eason, B. Noble, and I. N. Sneddon, "On certain integrals of Lipschitz-Hankel type involving products of Bessel functions," Phil. Trans. Roy. Soc. London, vol. A247, pp. 529–551, April 1955. *(references).*