International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 7 July 2022, pp: 375-383 www.ijaem.net ISSN: 2395-5252

Design and Implementation of Algorithms for Traffic Classification

Sandeep[1], Ritu kadyan[2]
[1]M.Tech Student, Department of Computer Science Engineering, Ganga Technical Campus, Soldha, Bahadurgarh.
[2]Assistant Professor, Department of Computer Science Engineering, Ganga Technical Campus

Submitted: 01-07-2022 Revised: 04-07-2022 Accepted: 08-07-2022

ABSTRACT

Visitors exam is an act of making use of the intrinsic excellent of organizational streams together with time, size, and reserving bundle to determine subtle statistics approximately it. The traffic exam strategy is used in connection with the extensive receipt of the encryption factor and content material, making it hard to acquire any facts approximately the float with the aid of breaking the substance.

In this postulation, we use site visitors assessments to accumulate complex information for numerous purposes and various packages. specifically, we take a look at special applications: P2P cryptographic cash, waft relationships, and tell packages. We want to alter the calculation of express site visitors examination this is exceptional to seize the herbal great of network traffic within the software for each of these packages. further, the cause of visitors investigations is distinct for each of these applications. mainly, in Bitcoin, we need to assess the power of Bitcoin visitors to inhibit sturdy materials along with management managed by the country and ISP. Bitcoin and comparable varieties of cryptographic cash assume a widespread a part of the digital commercial enterprise and other consider- based circulating frameworks as a result of their vital advantages of standard economic requirements, inclusive of open sales for internet groups round the world. As a result, it's far very important for shoppers and corporations to have strong revenues for his or her bitcoin sources. We examine business stone assaults for drift relations. The Venturing Stone is the host used by the attacker to hand over the traffic to cover his individual. In informing the utility, we check WhatsApp to inform the administrative traffic to determine whether it releases complicated facts, as an instance, the man or woman's character in sure discussions to the enemy who watches their traffic. This informing application safety is very primary

I. INTRODUCTION

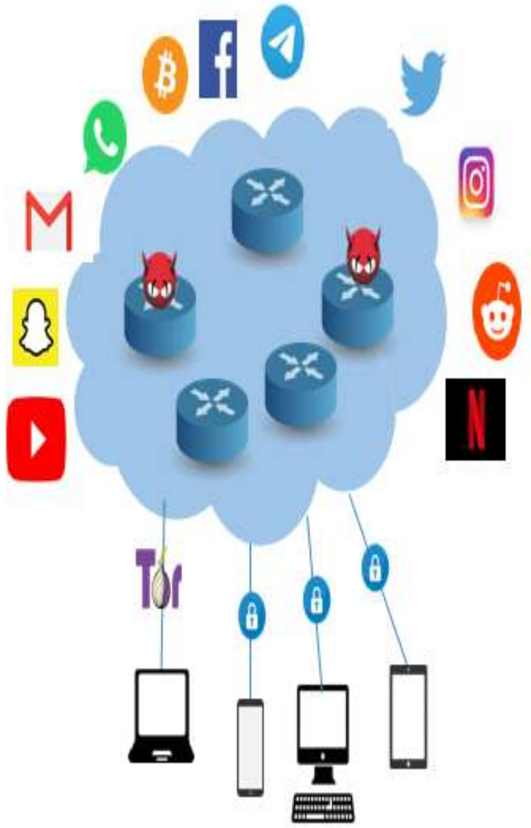
The net has made our lives extra trustworthy for each one in every of us. We keep at the net, interface with cherished ones, cowl our bills, read. It saves a ton of time and makes our lives an awful lot extra agreeable, but it comes on the price of our very own lives. We percentage a ton of facts at the net and our maximum sensitive facts is going thru the Internet and this represents some other chance

To assure the safety of Internet clients, community visitors is encoded, making it hard to split categorized facts from visitors. Notwithstanding the usage of encryption, community visitors releases sensitive records. The some distance and huge usage of encryption and similar substance disarray devices motivates contemporary techniques to extricate sensitive records from community streams, relying completely at the usage of visitors designs that do not fundamentally influence encryption and organization breaks, for example, bundle times. what's more, aspects rather than bundle items or titles; such examination is extensively remembered for transport investigation [42, 116, 22].

In this theory, we investigate traffic examination for an assortment of uses and purposes, specifically p2p digital currencies, informing applications, and bit by bit identification. In P2p digital forms of money, we concentrate on Bitcoin traffic to track down its unmistakable properties. We want to survey versatility to blockages by solid associations like legislatures. In informing applications, we investigate the WhatsApp informing administration to survey whether there is a protection spill in a singular association. In mysterious correspondence, we concentrate on stream relationship and plan calculations that permit network streams to be connected. Associating network streams is utilized to break the obscurity of mysterious associations of

Tor and such.

We utilize two essential methodologies in planning our calculations. To start with, we utilize measurable methodologies, in which we notice the stream examples of a stream or break a portion of its examples to remove more delicate information. Second, we use top to bottom review models to seclude the distinctive highlights of streams or to break a portion of its examples, like time. Beneath we make sense of the applications and approac in more detail communications are increasingly encrypted.

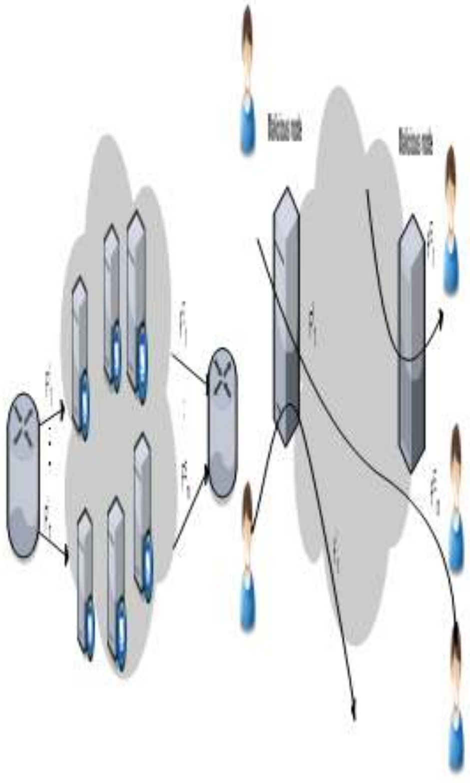


Applications of Traffic Analysis

In this postulation, we center around a few uses of traffic investigation: p2p digital forms of money, security of informing applications, and mysterious correspondences. We concentrate on Bitcoin traffic and survey its flexibility to blockage by strong associations like the ISP and the public authority. What's more, we break down the WhatsApp informing the administration and check if delicate data spill into its peak block. The security of information requests is a vital question because of their unlimited use. We also examine the flow relationship for unknown associations. The flow relationship is the most common way to find the associated flows and flows and in this way which connects the reflux of the organization and the flowing flows and transmitting the organization to break its insistence. postulation.

Stream relationship

Use of the traffic exam that we are considering is to connect these scrambled organizational flows as they go through unidentified intermediate servers. Stream relationship, we attempt to connect approaching and active organization streams. Connecting network streams is a significant issue in different security and protection applications. Specifically, it is notable that [116, 70] organization associations can be involved by contenders to break secrecy in Tor [45] and other obscurity frameworks [42, 82, 128, 127, 138, 72, 71, 70]. interconnection of transport types of information and result streams. It has likewise been proposed to connect network streams [70, 72, 71, 29, 142, 121, 130, 137, 46, 113] as a web search tool for cybercriminals



Stepping stone scenario

Bitcoin Identification

In addition, the grouping of Bitcoin traffic is more use of the characterization of the traffic that we think of. This is essential to study the versatility of Bitcoin to force areas for offices, including ISPs and States. Bitcoin and monetary standards based on comparable blockchain [98] were quickly adopted by buyers and the company because they can be used in web -based business and web business and web business and web business other trust-based dispersed frameworks. Bitcoin upholds $ 1-4.2 billion in exchanges each day and is developing consistently. Bitcoin and comparable virtual monetary forms offer critical benefits over customary e-monetary forms, including open admittance to the worldwide web based business foundation, low exchange charges, cryptographically upheld contracts [20], and administrations [95] and transnational tasks.

Given the significance of e-monetary standards, they should be impervious to government bans. That is, individuals who put resources into digital forms of money (by carrying on with work that depends on such monetary standards) need to ensure that their ISPs or states can't keep them from utilizing digital currencies assuming they choose to. For contention, consider what might occur in the event that China's Great Fire Wall chose to hinder all Bitcoin traffic for the time being.

In this postulation, we look at whether Bitcoin site visitors may be diagnosed via traffic exam notwithstanding the truth that it's miles burrowed through an encoded channel. sizes. Contrasted with exclusive conventions, we display that Bitcoin has novel visitors design styles despatched by using Bitcoin friends. the use of such first-rate elements different convention traffic via TOR [45] and three vehicles related by means of incorrect [111], especially ETP [48], docile [94] and OBFS4 [136] to assess our exposure. Classifiers.

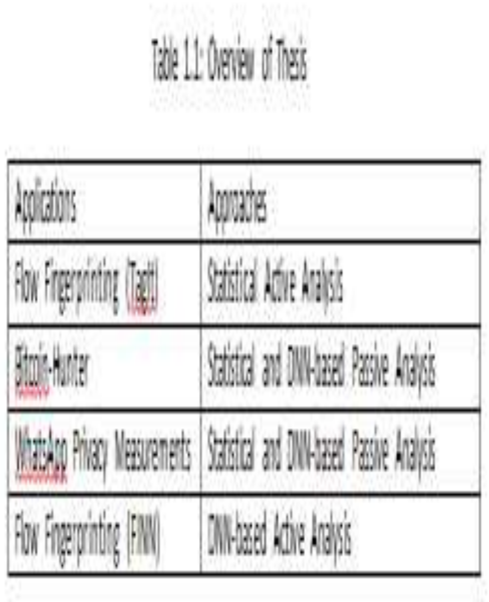


Table 1.1: Overview of Thesis

Applications	Approaches
Flow Fingerprinting (Tagit)	Statistical Active Analysis
Bitcoin-Hunter	Statistical and DNN-based Passive Analysis
WhatsApp Privacy Measurements	Statistical and DNN-based Passive Analysis
Flow Fingerprinting (FINN)	DNN-based Active Analysis

Sending SMS by using flexible administrators is high priced. especially, dynamic customers continually and a sum of 1.5 billion customers [12]. administrations allow clients to ship an collection of messages, which includes , message, sound, and records. especially, they make conditions for the buying and selling of strategically and socially sensitive subjects, which makes them inclined to being directed via robust designs like government.

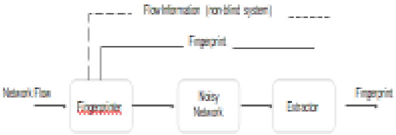
WhatsApp and comparative administrations supply begin to finish encryption to guarantee the safety of their customers. however, they validated that security regulations had Likewise, a name is in lots of instances misplaced from the system's call log. In 2019, WhatsApp changed into accounted for by means of common liberties activists and writers to have was an statement target using Israel's Pegasus spy programming. The adware authorised aggressors to get to passwords and on the spot messages from administrations, for example, WhatsApp [11]. Likewise, WhatsApp became critically impeded in China due to extended Communist celebration reconnaissance.

Here we take another heading to assess the safety of customers inside the WhatsApp informing administration. specially, we use traffic exam gadgets to evaluate whether or not an aggressor can get any delicate statistics by following WhatsApp visitors. users.

FLOW FINGER PRINTING

Flow fingerprints are an instrument for connecting dubious organization streams for a huge scope. In this proposal, we present the principal blind-streaming fingerprinting framework called TagIt. Our framework works by balancing unique finger impression signals into inert time stretches known exclusively to the gatherings getting the finger impression, through somewhat postponed bundles to the plans of the organization streams. We foster TagIt in a manner that is undetectable to a the regular contender, regardless of the normal obstruction in the organization, permits solid fingerprints to be gotten by genuine finger impression takers, yet who don't have a mystery unique mark key. TagIt utilizes randomization to counter different identification assaults, for example, multi-stream assaults. We assess the presentation and imperceptibility of TagIt through hypothetical examination, as well as reproductions and trials in a live organization. flow setting does not give any data on the flows between the gatherings to obtain fingerprints. The non -blind framework exchanges certain data on flows.

Figure 3.1: Single brand framework model of general flow. The visually impaired



The blind plans are quite more earth on earth. As examined in section 2.1 above, the traffic examination without discrimination proposes the calculation of correspondence o (1) and o (m) in a situation with n information and results flow captured by the members of printing the fingers. For a non -blind frame, for example, sophisticated, correspondence and calculation methods are o (n) and o (nm), individually. Note that, looking at the request for calculation between two unique brand frames, additional calculation expenses for each connection activity must be taken into account, as this can fluctuate for various executives (for example due to the use of various coding calculations). This is excluded from our calculation request examination on the grounds that similar relationship calculations used in a visually impaired framework can also be applied by a non -blind framework.

Based on stretching: there are two types of dynamic traffic examination frames sensitive to time: frames based on SPAN and IPD. The frame based on IP codes the print signal for the package delays between the beams, for example by modifying the IPDs independently. Again, the approach based on stretching refines the unique fingering sign with the quantity of plots appearing at a given duration. We use an extensible design for tagit. This is on the ground that Span Frameworks show much more anchored protection against normal modifications of the packages, for example, packet spill, reconditioning, package revision, etc., contrasting with frameworks based on IPD [72, 73, 70]. Changes. In this way, Tagit rests the progression of the printing beams of the fingers at a precise moment to obtain an impression of the fingers, which we call the unique brand stretches. The Tagit extractor develops the proportion of beams appearing at such stretching to obtain a unique brand.

Irregular information: the tagit -based SPAN -based approach makes levels of level waterproofing, as previously examined. Notwithstanding, Kiyavash et al. [80] show that the plans based on the scope can be inclined to an assault called a multi-FLUX assault (MFA). In this assault, the opponent brings together different flows from which the fingerprints are taken by using an extensible component and joins the flows to extend the ability to identify the impressive separations. The assault was worked at various periods of stretching of the plane in light of the factual diffusion of packages.

We created Tagit so that it is waterproof for the TIV assault, despite its conspire based on the section. More specifically, Tagit implies an irregular component for the choice the fingerprinting set the spans so that entering a similar unique finger impression two times in a similar stream will likewise bring about an alternate finger impression stream. In the examination of Section 4.5, we show that this powers TagIt to oppose the MFA by streamlining the factual appropriation of parcels over the accumulation of various TagIt streams.

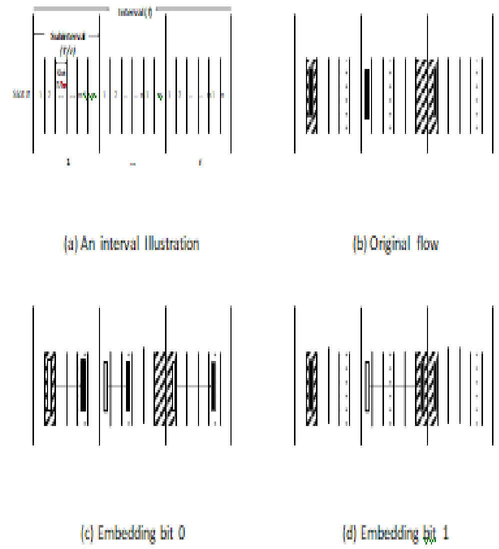
Encoding to forestall commotion: As referenced above, planning a dependable finger impression framework is more troublesome than a watermarking framework in light of the fact that the unique finger impression printing framework has information. We utilize two kinds of encoding that permit solid fingerprinting regardless of organization obstruction. To begin with, we utilize a redundancy code to oppose obstruction because of a straightforward organization jitter. Second, we utilize standard mistake remedy codes, (for example, decisions of coding boundaries. As displayed in the examination of Section 3.4, such encodings ensure the reliability of the TagIt fingerprint.t extraction.

Fingerprinting Scheme

In this segment, we examine the calculation utilized for TagIt unique mark network streams. As referenced above, TagIt is a time sensitive, stretch based plot, so it works by deferring a few bundles of stream with fingerprints for a specific measure of time. Underneath we depict the subtleties of the TagIt unique mark printer; Figure 3.2 shows the TagIt fingerprints

Partition the stream into time stretches. The finger impression gadget isolates the time pivot into a progression of time timespans T, the principal span beginning from 0 o <T offset time. That is, the I stretch contains bundles that show up in the time span [o + (I 1) T, o + iT]. The unique mark gadget utilizes the appearance season of the primary bundle in the up-and-comer stream as zero time.

Finger Determination of the printing beach. Tagit places fingerprints in streaming by postponing unique brand plots throughout the period, which we call the printing expanses. Suppose that a unique brand gadget intended to present coded L-chiffre 3.4. The unique Mark gadget uses the main time time time flow while the finger finger stretches and relegates the printing bits coded by LC to these racks (as examined later, we can enter various parts in a lonely



(a) An interval Illustration (b) Original flow

(c) Embedding bit 0 (d) Embedding bit 1

Figure 3.2: Place bits 0 and 1 with TagIt. Parcels ought to be moved to thicker subintervals to oblige 1, and to lighter subintervals to oblige 0.

tion capacities, n0 = (p0, p0, ..., p0) and n1 = (p1, p1, ..., p1)

), prior to beginning

0 1 r − 1 0 1 r − 1
the most common way of taking fingerprints and furtively imparting them to the extractor (s)

for m = 6.

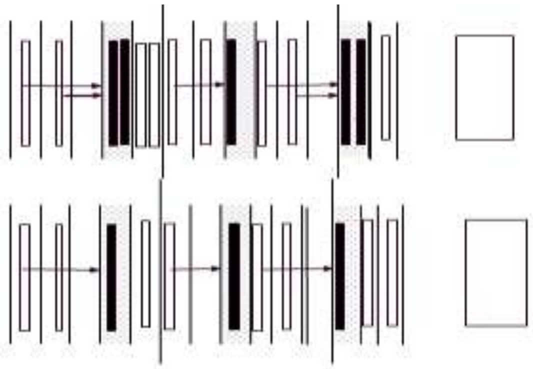
Zk = (pb (dk), pb (dk), ..., pb

(dk)) (3.1)

0 1 r − 1

Here b ∈ {0, 1} is the coded unique mark bit covered in the k-th stretch, and dk is the irregular seed (depicted later). Note that to build the obstruction of keys to full hunt assaults, we utilize different n0 and n1 capacities for various unique finger impression spans (this is broke down in Section 3.5).

Embed a unique finger impression bit. At last, unique mark pieces are embedded into the finger impression openings through the finger impression, which defers the bundles. That is, the k-th encoded finger impression bit is embedded into the k-span by postponing this stretch. packets



We **can** extract the embedded bit.

Figure 3.3: To ensure imperceptibility, TagIt fingerprinter just moves Rmove part of parcels into unique finger impression openings. Rmove relies upon the pace of the stream being fingerprinted (Rmove = 0.5 is delineated in the figure).

into the closest unique finger impression opening in their Zk (parcels are deferred forward, so bundles that show up after the last finger impression space of the stretch are not postponed). This is shown in Figure 3.2.

As we dissected in Section 4.5, deferring all bundles into the finger impression space for high velocity streams debilitates the imperceptibility include. That is the reason we defer just a part of the bundles into finger impression openings, Rmove. Assume Δ is the length between two back to back unique finger impression openings; the finger impression gadget just defers bundles from the last Δ R, move to the subsequent finger impression space of the intercellular space. This is displayed in Figure 3.3 (a). Note that we really want to choose this choice cautiously to accurately eliminate the unique mark. For instance, the piece set in Figure 3.3 (b) can't be taken out. We examine this boundary in Section 3.4.

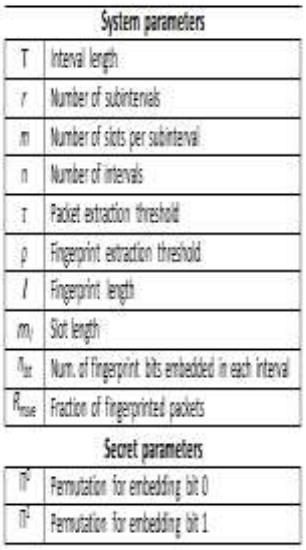
Void stretches For spans that we don't have a bundle for the unique finger impression, we basically disregard this span and hence lose the piece comparing to that span. Note that our selection of boundaries will be to such an extent that such unfilled spans are intriguing. Additionally, our utilization of encoding covers a portion of the missing pieces. On the other hand, the following non-void stretch can be utilized to put the proper piece; be that as it may, this expands the chance of full synchronization between the extractor and the unique finger impression, for instance, assuming a solitary parcel passes into a vacant space, the accompanying pieces are all lost in the extractor.

The fundamental limits are stealthily dispersed between the single brand and the extractor, and the remaining limits can be revealed to people in general.

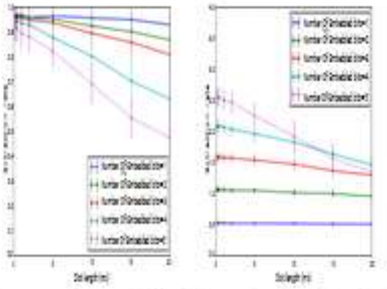
Expansion: Add a couple of pieces in every stretch

As talked about above, TagIt utilizes n0 and n1 to put bits 0 and 1, individually. We grow to n0, n1, ... NS-1 to have the option to put a bunch of progress capacities. S different message images, rather than just 2. At the end of the day, TagIt can embed

Table 3.1: Fingerprint Parameters.



System parameters	
T	Interval length
r	Number of subintervals
m	Number of slots per subinterval
n	Number of intervals
τ	Packet extraction threshold
ρ	Fingerprint extraction threshold
l	Fingerprint length
m_l	Slot length
n_{bit}	Num. of fingerprint bits embedded in each interval
R_{move}	Fraction of fingerprinted packets
Secret parameters	
π^0	Permutation for embedding bit 0
π^1	Permutation for embedding bit 1



(a) Extraction rate for various number of bits per interval (b) Average number of bits reliably extracted per second

Figure 3.4: Inserting multiple bits per interval.

$n_{bit} = \log_2 S$ bits of information per interval by using S numbers of permutation functions.

Bibliography

As Expected, the use of more exchange limits extends the complexity of the extraction, because the extractor should check more space cards. This increases in the same way the probability of extraction ankle: as we increase the quantity of replacement work, the probability of their pairing also built, causing extraction boys. This should be noticeable in Figure 3.4a, where the copy of the quantity of parts entered in each beach, moreover, manufactures the probability of a faux pas. parts constantly entered every second for different trading limits. (Note that acceptance of the stretch length, productivity is reduced with the fixed space length. The upper piece of the comparable spaces bet ween two guides

II. CONCLUSIONS AND FUTURE DIRECTIONS

Traffic analysis is the act of using the correspondence structures, for example, the times and objectives of the bump to summarize delicate data. In this postulation, we have investigated some uses of traffic exam and created and executed calculations for them

First of all, we focused on the current connection used in the discovery and disturbance bit by Bit de Tor and comparable unknown organizations. We have favored our calculations using two methodologies. First, we used a measurable methodology that broke float site visitors to summarize delicate data. 2d, we use a pinnacle and bottom evaluate to accumulate this records through guidance. We used a measurable manner to manage the calculation of the Plan Flux courting referred to as Tagit. Tagit uses a way based on quite a number handling virtual float fingerprints. all through enjoyment and assessments led in a planetary research established order, we display that our method is better than the framework of past fingerprints [70]. We additionally have a look at the imperceptibility of our frame the usage of a ok-S test and a multi-flux assault, and shows that our technique gives enough notion.

we have additionally favored a Finn flow dating technique for purposes inside and outside the organizational flows for fingerprints. Our framework modifies the package reviews to position the message in the glide. we're looking to show an organizational jig using our DNN -based shape to reliably separate our message introduced while the jig is going via the organisation. We present the presentation of our framework through fundamental examinations on Amazon EC2 and computerized sea poles.

We additionally focused on the electricity of Bitcoin traffic to be hampered by way of associations consisting of ISP or public authority. we've got portrayed examples of Bitcoin site visitors to find its undoubted features to plot a customized classifier to differentiate Bitcoin. way to huge analyzes, we exhibit how our classifiers can understand bitcoin in backstage traffic and digs via confusion channels.

ultimately, we measure the security of the character correspondence of WhatsApp and the spill of its categorized purchaser information. We perform estimates on WhatsApp informing the administration and decompos its spills with potential information thanks to the survey on traffic. We collect individual correspondence information on WhatsApp and keep ideas calculations to assess your privacy. Whenever traffic WhatsApp goes through a VPN, we also assess the exposure of our classifier and emphasize that more founded countermeasures should prevent the traffic survey. attack.

Bibliography

[1]. China blocks whatsapp, broadening online censorship. https://www.nytimes.com/2017/09/25/business/china-whatsapp-blocked.html.

[2]. Cluster analysis. https://en.wikipedia.org/wiki/Clust er analysis.

[3]. Digitalocean. https://www.digitalocean.com/.

[4]. Libnetfilter queue. http://www.netfilter.org/projects/libnetfilter_queue.

[5]. Messaging Application Stat. https://www.statista.com/statistics/258749/most-popular-global-mobile-messenger-apps/.

[6]. Messaging applications. https://en.wikipedia.org/wiki/Messaging apps.

[7]. Mtproto mobile protocol. https://core.telegram.org/mtproto.

[8]. Russia asks telegram to cooperate. https://www.seattletimes.com/nation-world/russian-court-telegram-app-must-cooperate-with-spy-agency/.

[9]. Whatsapp discovers ’targeted’ surveillance attack.https://www.bbc.com/news/technology-48262681.

[10]. Whatsapp encryption overview: Technical white paper. https://scontent.whatsapp.net/v/t39.8562-34/122249142_469857720642275_2152527

586907531259_n.pdf/WA_Security_WhitePaper.pdf?ccb=1-3&amp;_nc_sid=2fbf2a&amp;_nc_ohc=HurtY7LryYEAX_sl4zy&amp;_nc_ht=scontent.whatsapp.net&amp;oh=cbbd2e9a5c46fc5cd26f55996624f520&amp;oe=608DBF19.

[11]. Whatsapp says indian journalists were spied on. https://thewire.in/tech/ israeli-spyware-was-used-to-spy-on-indian-activists-journalists-says-whatsapp.

[12]. Whatsapp statistics. https://99firms.com/blog/whatsapp-statistics/.

[13]. Whatsapp web. https://web.whatsapp.com/.

[14]. Whatsapp wikipedia. https://en.wikipedia.org/wiki/WhatsApp.

[15]. Wonder Shaper. https://github.com/magnific0/wondershaper.

[16]. BotMosaic: Collaborative network watermark for the detection of IRC-based botnets. Journal ofSystems and Software, 2013.

[17]. M. Abadi, A. Agarwal, P. Barham, E. Brevdo, Z. Chen, C. Citro, G. S. Corrado, A. Davis,J. Dean, M. Devin, S. Ghemawat, I. Goodfellow, A. Harp, G. Irving, and e. a. Michael Isard.TensorFlow: Large-scale machine learning on heterogeneous systems, 2015. Software available from tensorflow.org.

[18]. G. Aceto, D. Ciuonzo, A. Montieri, and A. Pescap`e. Mobile encrypted traffic classification using deep learning. In Network Traffic Measurement and Analysis Conference, TMA 2018, Vienna, Austria, June 26-29, 2018.

[19]. G. Aceto, D. Ciuonzo, A. Montieri, and A. Pescap`e. MIMETIC: mobile encrypted traffic classification using

[20]. k. claffy. Internet traffic characterization. PhD thesis, UC San Diego, Jun 1994.

[21]. M. Cotacallapa, L. Berton, L. N. Ferreira, M. G. Quiles, L. Zhao, E. E. N. Macau, and D. A. Vega-Oliveros. Measuring the engagement level in encrypted group conversations by using temporal networks. In 2020 International Joint Conference on Neural Networks, IJCNN 2020,Glasgow, United Kingdom, July 19-24, 2020. IEEE, 2020.

[22]. S. E. Coull and K. P. Dyer. Traffic analysis of encrypted messaging services: Apple imessage and beyond. Computer Communication Review, 44(5):5–11, 2014.

[23]. M. Crotti, M. Dusi, F. Gringoli, and L. Salgarelli. Traffic classification through simple statis- tical fingerprinting. Computer Communication Review, 2007.

[24]. G. Danezis. The traffic analysis of continuous-time mixes. In Privacy Enhancing Technologies, 4th International Workshop, PET 2004, Toronto, Canada, May 26-28, 2004, Revised Selected Papers.

[25]. A. P. Dempster, N. M. Laird, and D. B. Rubin. Maximum likelihood from incomplete data via the EM algorithm. Journal of the Royal Statistical Society: Series B, 1977.

[26]. C. Dewes, A. Wichmann, and A. Feldmann. An analysis of internet chat systems. In Pro- ceedings of the 3rd ACM SIGCOMM Internet Measurement Conference, IMC 2003, Miami Beach, FL, USA, October 27-29, 2003. ACM.

[27]. R. Dingledine, N. Mathewson, and P. F. Syverson. Tor: The second-generation onion router. In Proceedings of the 13th USENIX Security Symposium, August 9-13, 2004, San Diego, CA, USA.

[28]. D. L. Donoho, A. G. Flesia, U. Shankar, V. Paxson, J. Coit, and S. Staniford. Multiscale stepping-stone detection: Detecting pairs of jittered interactive streams by exploiting maxi- mum tolerable delay. In RAID, 2002.

[29]. R. Durrett. Probability: theory and examples. Cambridge university press, 2010.

[30]. K. Dyer, S. Coull, T. Ristenpart, and T. Shrimpton. Protocol Misidentification Made Easy with Format-transforming Encryption. In CCS, 2013.

[31]. K. P. Dyer, S. E. Coull, T. Ristenpart, and T. Shrimpton. Peek-a-boo, I still see you: Why efficient traffic analysis countermeasures fail. In IEEE Symposium on Security and Privacy, SP 2012.

[32]. J. A. Elices and F. P´erez-Gonz´alez. The flow fingerprinting game. In 2013 IEEE International Workshop on Information Forensics and Security, WIFS 2013, Guangzhou, China, November 18-21, 2013.

[33]. J. A. Elices and F. P´erez-Gonz´alez. A highly optimized flow-correlation attack. CoRR, 2013.

[34]. J.Erman, M. F. Arlitt, and A. Mahanti. Traffic classification using clustering algorithms. In Proceedings of the 2nd Annual ACM Workshop on Mining Network Data, MineNet 2006, Pisa, Italy, September 15, 2006.

[35]. J. Erman, A. Mahanti, and M. F. Arlitt. Internet traffic identification using machine learning. In Proceedings of the Global

Telecommunications Conference, 2006. GLOBECOM '06, San Francisco, CA, USA, 27 November - 1 December 2006. IEEE.

[36]. J. Erman, A. Mahanti, M. F. Arlitt, I. Cohen, and C. L. Williamson. Semi-supervised network traffic classification. In L. Golubchik, M. H. Ammar, and M. Harchol-Balter, editors, Proceed- ings of the 2007 ACM SIGMETRICS International Conference on Measurement and Modeling of Computer Systems, SIGMETRICS 2007, San Diego, California, USA, June 12-16, 2007.

[37]. J. Erman, A. Mahanti, M. F. Arlitt, I. Cohen, and C. L. Williamson. Offline/realtime traffic classification using semi-supervised learning. Perform. Eval., 2007.