A Novel Approach to Detecting DNS Tunnels Using Throughput Estimation

Michael Himbeault (mike.himbeault@gmail.com) and
Jacky Baltes (jacky@cs.umanitoba.ca)

University of Manitoba

Abstract. DNS tunnels represent a clear and common threat to network security by bypassing existing security and administrative controls. The ability for DNS tunnels to transmit arbitrary data via conforming DNS packets makes them difficult to detect. This work describes a novel entropy based approach to detecting DNS tunnels. The approach is efficient and can process more than 2 Gigabits per second per second on commodity hardware. Testing shows that our approach achieves a ninety percent reduction in false-positive rates than the next best achieving up to 25% better processing performance.

Keywords: intrusion detection, APT, DNS, entropy, NIDS, network analysis

1 Introduction

Covert tunnels circumvent network control systems such as firewalls, proxies, and/or content filters. The use of covert tunnels may be benign [14] but is often malicious (e.g., theft of sensitive data, infiltration of data, or as control channel for malware) [11]. A common method for establishing a covert tunnel is via the Domain Name Services (DNS) protocol, which translates host names (e.g., www.google.com) into IP addresses (e.g., 173.194.33.148). DNS provides an integral service to the Internet and thus cannot be blocked easily. Therefore, efficient and accurate detection of DNS tunnels on a busy network link is an important problem in network security.

A common method for detecting of malware or network breaches is by comparing observed network data against a library of known security threats, so called signature based approaches. However, the detection of DNS tunnels via traffic signatures is inflexible and unusable in zero-day attacks. Therefore, some researchers proposed character frequency based approaches or similar approaches [4].

Our method assumes that DNS tunnels move more information than a normal domain but do not necessarily do it by moving more bytes or packets than a benign domain. This distinction is important since, on a busy network, a large content or service provider such as Google, Amazon, Facebook or Twitter may make up orders of magnitude more DNS traffic by byte count than a DNS tunnel. A brief treatment of the

effects of DNS caching on the number of bytes observed in repeated query strings is given in Sect. 5.1. Our method uses an entropy based estimate of the amount of information being transmitted via DNS queries to detect DNS tunnels.
Our method can detect DNS tunnels in as few as ten packets (as shown in Sect. 6.1) and works robustly in difficult real-world detection environments (i.e., environments that contain a great deal of non-tunnel traffic as well as benign uses of DNS). Detection performance on commodity hardware is shown to scale to greater than two gigabits of UDP port 53 throughput per second in a performance-oriented C++ implementation. Section 6.3 compares the processing performance of various approaches from the literature to our method and shows that our method has better performance. Section 7 compares the detection performance of our approach to its peers, demonstrating that our approach also provides superior detection performance.

2 Background

2.1 Covert Channels

Covert channels are methods of communication that use non-standard means of communication typically for the purpose of evading detection and/or blocking by the existing security infrastructure. Covert channels may utilize portions of an existing protocol[3] or communication channel, or they may find ways of transporting information utilizing a completely new medium. An example of the latter is called a *timing channel*[22], which can utilize the timing between packets to convey information. A timing channel carefully controls the timing between packets sent to a remote server to encode information, thereby utilizing a method of communication that is not utilized by any standardized protocol or communication method.

2.2 DNS Tunnels

DNS tunnelling is the method by which arbitrary data is transferred over the same channels as DNS. DNS tunnels come in one of two primary types: raw, or conforming.

Raw DNS Tunnels Raw DNS tunnels do not attempt to mimic or conform to the DNS specifications, and simply attempt to utilize the fact that UDP port 53 is often left relatively uncontrolled in firewalls. Raw tunnels attempt to exploit this by transmitting arbitrary traffic using UDP port 53 packets with arbitrary payload [1]. This is the most efficient exploitation of the ubiquity of DNS as it incurs the lowest amount of overhead, both computationally and in terms of network throughput. The trade off for this efficiency is that it is the least conforming and the most likely to get stopped by either a firewall or a proxy. In the situation where all DNS queries are forced to be proxied through a dedicated DNS server, raw DNS tunnels will fail to operate as expected.

[1] Iodine demonstrates this behaviour when operating in its raw transport mode

Conforming DNS Tunnels Conforming DNS tunnels produce DNS packets that conform to all appropriate specification and RFC documents and, as far as any DNS server is concerned, the traffic generated is valid DNS traffic. These tunnels incur the highest computational and throughput overhead, but have the advantage that detecting and blocking them is a very difficult process. The detection of this type of DNS tunnels is the topic of this work. This type of tunnel is capable of operating in almost any environment, even those with very strict firewall and proxy policies.
Conforming DNS tunnels operate by embedding the data for transmission into the query string and response, requiring a modified, non-conforming, server on one end of the connection and a piece of software on the client end. Typically these types of DNS tunnels have one endpoint that is controlled by the tunnel user, with that controlled endpoint running dedicated server software. The client and server software are responsible for transforming arbitrary information to and from DNS queries and responses.

DNS Tunnel Software Some existing DNS tunneling software currently available is OzymanDNS[19], Iodine[10], Dns2tcp[8], DNScat[18] and DeNiSe[12], and PSUDP[2]. Each of these have slightly different operational characteristics, but they all aim to do the same thing which is transmission of arbitrary data over DNS.

3 Review of the State of the Art

The solutions that exist to date to detect DNS tunnels generally make very little use of complex and static signatures, but rather attempt to exploit a characteristic trait or property that the DNS tunnel will exhibit. If a tunnel can be crafted to not exhibit that feature, then those detection strategies will normally fail in their detection.
The SANS Institutes's InfoSec Reading Room published a report on the design and detection of DNS tunnels[13]. The report covers a very wide variety of topics including background information, tunnel-specific information, technical information, existing applications, detection techniques, detection implementations, and a sample detection scenario. This report is exceptionally good reading as a primer on the topic.
The sample detection scenario employs an analysis technique very similar to the technique that will be outlined in Sect. 5.
(Karasaridis, 2006)[16] proposes and evaluates mechanisms that use network flow data to detect DNS anomalies including cache poisoning and tunnels. The authors are able to observe considerable changes in their cross-distribution entropy measurement during the onset of the Sinit virus in their real-world data. This approach is discussed in additional detail in (Roolvink, 2008)[21].
(Born, 2010)[1] discusses a way of using javascript in a web browser to exfiltrate data from a network, while [3] discusses a novel way of crafting a DNS tunnel that exploits the nature of a DNS packet and the ability

to create unused space in the packet in which arbitrary data can be stored. [4] discusses a method of detecting DNS tunnels by examining character and n-gram frequencies in the names that are being queried for. [5] demonstrates the effectives of data visualization when attempting to detect a DNS tunnel using a custom visualization engine using the character frequency analysis proposed in [4]. If a DNS tunnel can be crafted such that its character frequencies are distributed sufficiently close to those of legitimate DNS names, then it is possible to hide a DNS tunnel from this type of analysis.

(Butler, 2011)[6] proposes a *codeword mode* of communication over DNS where a specific lexicon is chosen that allows the two endpoints to communicate with each other. Each word in the dictionary has a particular meaning that is understood by both endpoints.

(Romana, 2007)[9] discusses their analysis of DNS data on a large campus network using the output of a DNS resolver's query logging as their input. The authors estimate the entropy of the source IP address (of the DNS query) and the queries themselves, and perform analysis based on that digestion.

(Thomas, 2011)[24] proposes and evaluates the efficacy of a Field Programmable Gate Array (FPGA) based solution for detecting malicious DNS packets on a high throughput network link using a hash-based blacklist of disallowed domains for accept/reject decisions.

(Dietrich, 2011)[11] examines the use of DNS for command and control of botnets based on the reverse engineering of the *Feederbot* botnet application. Based on the lessons learnt from Feederbot, the authors applied their methods to other real-world traffic and detected other botnets that also use DNS as their command and control medium.

(Paxson, 2011)[17] is a slide deck that discusses the author's searches through large campus networks for DNS tunnels in the wild. The author proposes an approach for detecting DNS tunnels that is similar to our method in that it examines the approximate amount of information transferred per domain and/or subdomain. However, the author, instead of utilizing exact entropy measures, uses *gzip*[2] to estimate the amount of information transferred to a domain in a given collection of queries.

jhind[15] gave a presentation at DefCon 17 that discusses the use of artificial neural networks to identify DNS tunnel traffic. The author successfully detected DNS tunnels as produced by several software packages (Iodine, Ozymandns and Dns2tcp) using the described approach.

Static signatures exist for at least three common network anomaly detection engines (Snort[7], Proventia[20], and TippingPoint[3]) engines, with others likely offering similar functionality.

---

[2] *gzip* is a compression utility that compresses input streams such as archives or other files.

[3] TippingPoint does not make information about its filters available publicly, however a personal correspondence with a TippingPoint user revealed that filters 9932 and 9938 trigger on the application data contained in DNS packets generated by Ozymandns.

4 Problem Statement and Evaluation Criteria

4.1 Detailed Problem Description

DNS tunnel detection is a complicated task made more difficult by the fact that DNS tunnel traffic can appear to be completely legitimate network traffic that conforms to all standards and restrictions. It need not violate any established standards or conventions, which makes it difficult to detect against the background of normal DNS traffic based on testing for violations.
For this reason an efficient method of detecting DNS tunnels is required that can effectively detect a DNS tunnel against normal DNS traffic with a low false-positive rate and that must not be susceptible to existing methods of circumvention.

4.2 Solution Evaluation Criteria

The objectives that must be met for an approach to have successfully solved the problem posed are:

- Successfully discern tunnel traffic generated from existing tunnel applications and theoretical tunnel traffic (built using additional parameters to attempt to hide from known detection methods) from a baseline of normal traffic.
- Be resistant to known obfuscation methods compared to existing detection methods.
- Be able to operate at high speed on general purpose, easily obtainable hardware.

We evaluated our approach against these criteria to determine whether or not it can be considered an improvement on the state of the art for this type of detection.
Item 1 was validated by comparing the chosen approaches against our approach in a relative scoring fashion. Methods were compared to their peers for relative detection performance, and improvement therein, in the various test scenarios. Methods were scored based on false positive rates, with lower rates being more desirable.
Item 2 will be tested using a next-generation tunnel and referred to as `next-gen`, that simulates what DNS tunnelling applications may look like in the future. The primary difference is that output of this tunnel is set to match the character frequency distributions of normal DNS queries. Due to the implementation details of the next-gen tunnel, there is no server-to-client transfer direction for that tunnelling application.
Item 3 will be tested by comparing the approaches when implemented on a common Python framework to produce a level playing field of performance.

5 Our Detection Method

Our method examines the information theoretical properties of the DNS queries to each domain, thus retaining the flexibility to filter and alert per domain as opposed to more generally on the set of all DNS queries.

5.1 Theoretical Basis

Assumptions Our detection approach makes certain assumptions about the nature of DNS tunnels in order to effectively detect them. The primary assumption made is that DNS tunnels move more information than a normal DNS subdomain, with a very particular meaning of *data* that goes beyond simply counting bytes or the number of queries. The concept of the amount of information transferred to a DNS domain considers the entropy of the queries as a whole, and not just the characters/data that make up a query. The list of assumptions follows:

- DNS tunnel applications use the queries themselves to transport information from the client to server.
- There are more unique queries per domain (or subdomain) proportional to the amount of information transferred from the client to the server.
- Even in server-to-client communication, acknowledgements must be sent from the client to the server, with the acknowledgement encoded in the query string.

The primary assumption, in the language of DNS queries, is that DNS tunnels will cause more unique DNS queries to a domain (or subdomain) than benign traffic. If a DNS tunnel is able to construct its network traffic in such a way that this assumption is no longer true, then our approach will be ineffective in detecting it.

Theory In a large internet provider network, it is possible that there could be many copies of the same DNS query - say *google.com* - each of which would count towards the total number of bytes or queries transferred to/from that domain. This repitition has detrimental effects on the metric calculated for popular domains when using a naive detection approach (e.g., counting bytes or queries to/from a domain).
In order to work around this, our approach instead uses entropy to measure the amount of information moved in the queries to a domain or subdomain. By considering queries as atomic objects, and maintaining a tally of the queries to a domain, and their counts over an interval, a probability distribution function (PDF) is generated. By computing the entropy of this PDF, a basic measure of throughput is achieved. However, since there is value in the capturing the length of the queries that were sent (since longer queries are moving more bytes than shorter ones), the entropy is multipled by the average query length (in bytes) over that interval. This metric, which we call the Domain Length-Weighted Entropy (DLWE), is our primary mechanism for detecting DNS tunnels.
With this new throughput measure, the approach considers intervals of time and computes the amount of estimated to be moved by each domain over that interval. By sorting all domains by their information throughput, the heavy-hitters can be examined in each time interval. White-listing can be used to prevent false alarms for known benign DNS tunnels. As will be shown in Sect. 6.3, this approach is capable of processing packets nearly as fast as a naive approach with equivalent or better detection performance (see Sect. 7).

The Effect of DNS Caching on Detection Effectiveness Because the packet capture was done in an environment where a large portion of the clients use one of only a few different DNS servers, the effects of caching will cause the naive approach to have far better detection performance than if this were not the case.

In order to grant some context to the effects that DNS caching has had on the naive method's performance, a simple comparison is offered. Data was taken from a home network serving five computers and smartphones, with DNS traffic logged over a twenty-two day period to match the time frame of the capture for real world data. Over that twenty two day period, *www.google.com* was queried 5645 times compared to the 268842 times the same query was seen in the real world traffic capture. It is important to modulate these values by the number of hosts that the real world traffic represents, which is on the order of approximately thirty thousand, or six thousand times the number of hosts the home network was supporting. Approximately scaling the home network by a factor of six thousand results in an estimated three million queries to *google.com* occurring in the real world traffic, of which only a twelfth actually appeared in the capture due to DNS caching.

A small sample of data was collected from Merlin's[4] caching DNS servers which represents *every* DNS query made of them, regardless of whether those queries were served from the cache or not. Figure 1 shows the effects of query caching on the repetition counts of queries in networks. The home network, mentioned above, as well as Merlin's network are represented in order to demonstrate scale. The horizontal axes represents the count of queries, normalized as a proportion of the maximum count.

Each plot was built by tallying the DNS queries in each capture, sorting by count, and then dividing by the largest count. The y-value on the plot then represents the proportion of unique queries that had a count greater than xM_d where x is the horizontal value and M_d is the maximum count for that particular dataset.

From the plot it is evident that the queries in an uncached environment occur over two orders of magnitude more frequently than in a cached environment. This increased occurrence in an uncached environment would have a strongly visible impact on the naive metric's ability accurately detect DNS tunnels.

As can be seen from the our method's underlying mechanisms, the DNS caching actually provides a *more pessimistic* detection environment compared to the uncached environment. Unlike the naive method, whose detection performance results will not be applicable in an uncached environment, our method can be expected to perform better in an uncached environment than in the testing in Sect. 7.1.

[4] Merlin is a small ISP that supplied the primary data set for the testing.

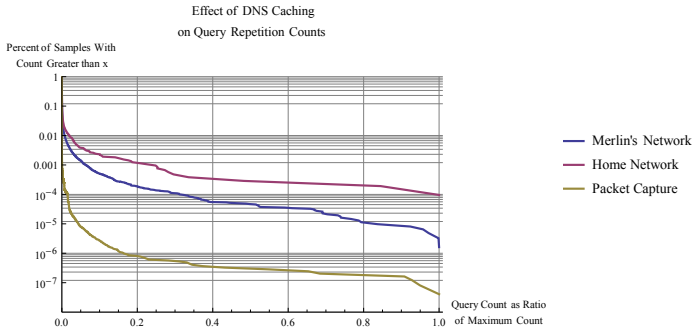


Fig. 1. Shows the trends for DNS query counts in networks with and without caching. The axes are normalized to account for the fact that the real world data has much more data than the home network. By normalizing the query counts, it is possible to perform a direct comparison.

6 Detailed Testing Methodology and Processing Performance

A collection of tests were run on several detection methods, demonstrating the performance of our method when compared to existing methods from the literature. The detection methods chosen for comparison are

- The n-gram detection proposed by Born[4] because it is well defined and was the most prevalent approach found during the literature search. Additionally, the approaches built on this technique claim reasonable success in detecting DNS tunnels.
- The use of *gzip* on domain and subdomain packet data as proposed by Paxson[17] because it involves looking at data that is very similar to the proposed approach, but makes use of different methods for measuring the data throughput.
- A naive approach that simply measures the volume (in number of characters in the query strings) of packets per domain/subdomain in an attempt to illustrate that simple volume of queries is a highly inadequate approach, and that more sophisticated approaches can perform considerably better.

The collection of methods was put through several tests in an attempt to demonstrate their performance in average (using existing implementations) and worst case scenarios. All of the tests involving traffic generation were performed in a virtual environment of two Linux-based virtual guests directly connected via a virtual network on a single physical host. The tunnelling applications were communicating between the virtual hosts, transmitting content from the high entropy source `/dev/urandom` under Linux.

6.1 Situational Performance Goals

Determining a Baseline Through cooperation with Merlin, an educational Internet Service Provider (ISP) in Manitoba, DNS traffic was collected over a period from Thursday November 4 2010 until Friday November 26 2010. The hosts responsible for the DNS traffic observed include several dozen school divisions totalling tens of thousands of individual computers. The capture includes just over one billion packets destined to, or sourced form, UDP port 53 (the standard DNS port).
This captured traffic will be used to determine a baseline distribution to which the metrics produced on isolated tunnel traffic can be compared. This baseline will provide context in order to determine if a method is able to detect a tunnel with sufficiently high certainty.
It is assumed that the incidence of tunnels in this baseline traffic is sufficiently low that it can be discounted. This assumption may not be perfectly accurate due to to reasons indicated in the introduction. The effect of tunnels present in the real world traffic given the assumption that there are none will result in a more pessimistic environment for testing, since a portion of the false positive rate that the detection approaches will suffer may actually be due to the classification of existing traffic as a tunnel, and not due to misclassification.

Existing Implementation Detection This test will involve the two hosts communicating at varying throughput rates using the chosen existing DNS tunnel implementations. The throughput rates will scale from as little as several bytes per second, to as high as the tunnel applications can support. The wide range of throughputs used is done to give an indication of how the detection methods scale with tunnelled throughput.
The existing implementations chosen for testing in this section are Iodine[10], DNScat[18], and DNS2TCP[8]. Iodine is chosen due to the fact that it provides a full VPN solution without additional work by the user. DNScat is chosen due to being written in Java and so runs on multiple platforms without the need for a compiler or other complex dependencies that the user must obtain. DNS2TCP is chosen since it does not require root access, and is written in C indicating potentially better throughput than other mechanisms.
Instead of generating a large number of distinct events that will be detected (or not) resulting in a ROC plot, rather a much smaller number of prototypical events were produced. In essence, detection methods will be scored for false-positive rate and ranked against each other in order to determine a relative rating and ranking. The relative performance comparisons allow for a more contextual performance analysis to be done between two methods that perform very similarly.

6.2 Tunneling Application Throughput

The tunnelling applications used during the evaluation were subjected to different rates of traffic in both client-to-server and server-to-client directions. For each tunnelling application, sixteen captures were performed

at each of the following target throughput rates (in bytes per second) in each direction (client-to-server and server-to-client where applicable):
10, 25, 50, 100, 250, 500, 1000, 2500, 5000, 10000, 25000, 50000, 100000, 250000, 500000, 1000000
The rates stop at ten bytes per second for practical reasons. It is considered reasonable to assume that tunnels with a throughput rate lower than this are ineffective at transmitting sufficient data to be practically useful in many situations. As will be seen in Sect. 7, throughput rates lower than ten bytes per second would quickly become lost in normal DNS traffic for even the most discerning detection methods.
Due to implementation details of the applications, and of the next-gen tunnel, not all applications were able to transmit traffic at the target rate. Figure 2 shows how the various tunnelling applications responded to various input rates, plotting their actual rate of ingestion of input and the observed number of characters of query output they generated on the network. The next-gen tunnel was not tested in a server-to-client direction since it does not implement that functionality.

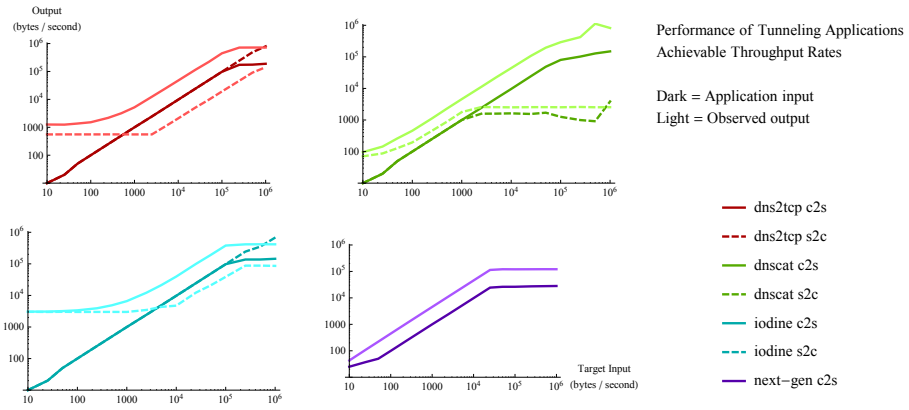


Fig. 2. Shows the scaling behaviour of DNS tunnelling applications as the input rate is scaled up. Note that not all applications are capable of transmitting data at the rate they are given data, which is visible as a plateau on the right-hand-side of each plot.

6.3 Detection Method and Python Interpreter Processing Performance

Python has several interpreters available freely in addition to the standard interpreter (for this discussion, the standard interpreter will be referred to as Cython). A notable alternative, called PyPy, is a Python interpreter written in Python itself that contains just-in-time compilation (JIT) mechanisms that Cython does not have. PyPy can offer an order of magnitude or better speedup[23] in some workloads. Figures 3,

4(a), and 4(b) show the performance of the various detection methods over aggregate tunnel and real-world data on both PyPy and Cython.

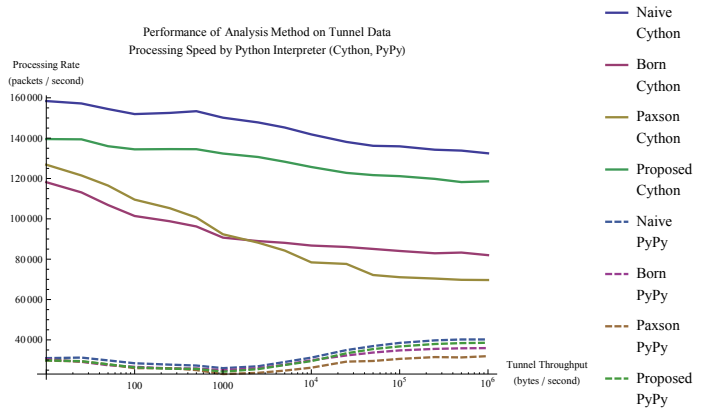
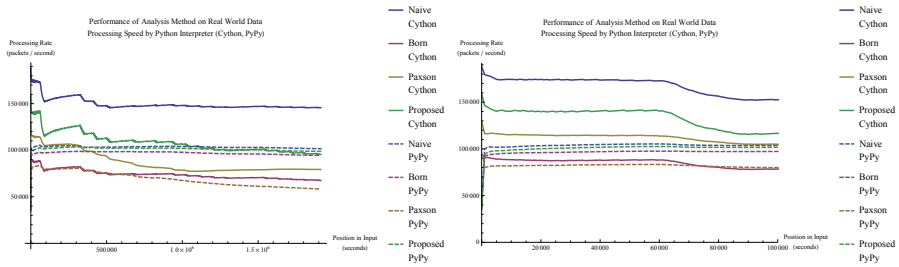


Fig. 3. This plot shows the performance of the detection methods and Python interpreters over the aggregate tunnel data. The output is packet processing rate as a function of the target input rate (rate at which the tunnels are transmitting traffic).



(a) Full data set (b) Early time

Fig. 4. Performance of Analysis Method and Python Interpreter on Real World Data

Figure 4(a) shows the performance of the detection methods and Python interpreters on real world DNS traffic. The output is packet processing performance as time progresses and more packets are processed by the script.

Figure 4(b) is identical to Fig. 4(a) but restricts the time displayed to the first one hundred thousand seconds. The 'spool up' of the JIT portion of PyPy is noticeable in the very early time-scales.

Figure 5 attempts to represent the performance of the various detection methods and Python interpreters as more tunnel data is moved through them per interval. Their horizontal axes are the actual data input rate (see 6.2), and the vertical axes indicate the processing rate (in packets per second).

In Fig. 5 the legend requires some additional context. The plot legends contain labels of the form *dns2tcp c2s Cython* which contains three distinct pieces of information. The first word indicates which tunnelling application being one of DNS2TCP, DNSCat, Iodine, or the next-generation simulated application which is indicated by a name of `next-gen`. The second word indicates whether the data being moved over the tunnel is being transferred from the client to the server (`c2s`) or from the server to the client (`s2c`). The final word indicates which Python interpreter is being used.

There are fourteen lines on each figure, each corresponding to a Python interpreter, tunnel application, and data transfer direction triple. The solid lines correspond to runs made under the Cython interpreter and dashed lines indicate the use of the PyPy interpreter.

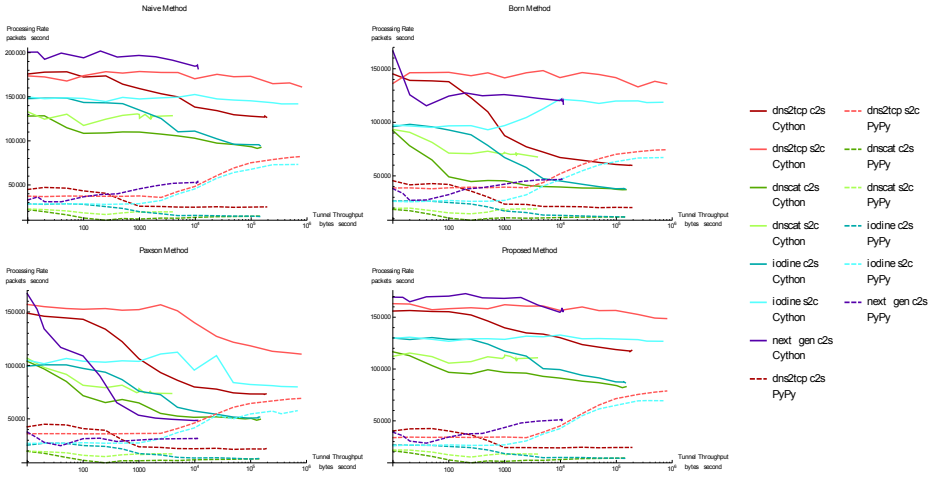


Fig. 5. Performance of all methods on separated tunnelling application data, showing processing rate as a function of input rate.

Our approach shows performance characteristics and trends that match the naive approach far more closely than either of the other two approaches. There is minimal degradation in performance for most of the tunnelling applications, and almost all of the samples under the Cython interpreter are above one hundred thousand packets per second.

It is instructive to observe that PyPy's performance overall is considerably lower than Cython on tunnel data, but as is shown in Fig. 4(a), this is not the case on real-world data.

6.4 Processing Performance Conclusion

When evaluating the performance of the detection methods on real-world data, in all cases the naive method is the fastest, followed by our approach, Born's method, and Paxson's method in order.
When operating on tunnelling application traffic, the average performance of the methods (averaged over all tunnels and cases) can be seen in Fig. 3 where the our method and the naive method both perform well, maintaining processing rates in excess of one hundred twenty thousands packets per second. Born's and Paxson's approaches both suffer severe degradation of performance as throughput increases, resulting in final processing rates well below one hundred thousand packets per second.

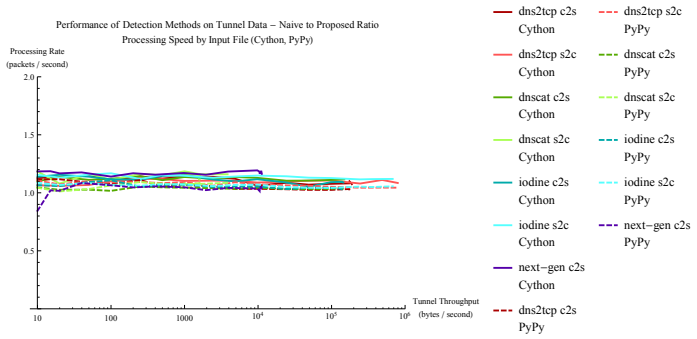


Fig. 6. The ratio of the performance of the naive method to our method on separated tunnelling application data, with the vertical axis showing the speedup of the naive method over our method.

When the ratio of the performance of the naive method to our method is examined, a clustering very close to a fixed value is observed as in Fig. 6. This indicates that much of the performance degradation, and potentially other performance characteristics, of the two methods are dominated by the common scaffolding and/or the Python interpreter as opposed to the underlying methods or their implementation.
Through this examination, it has been shown that our method outperforms both methods from the literature by a considerable margin and comes very close to matching the naive method in performance in many cases.

7 Tunnel Detection Evaluation

In order to obtain the metrics used in this section, tunnel application and real world data was separated into adjacent ten second windows for processing. The distribution of metrics across these windows is computed and used to produce the plots for real world data as well as indicative representative values for tunnel applications.

When examining the distribution of metrics produced by tunnel applications, it was discovered that the metrics were clustered extremely tightly around the mean. The relative standard deviation for the various tunnel applications, transfer directions (server-to-client or client-to-server) are given as a function of input rate for each of the detection methods in Fig. 7 . These plots show that the clustering around the mean for these metrics is so tight that a standard receiver operating characteristic (ROC) plot would be of little additional value since the true and false positive rates are dependant on the value ranges that the metrics take. Since the range of values that the metrics take on is so limited, the differences between a low and high percentile in true and false positive rates would be minimal to statistically insignificant.

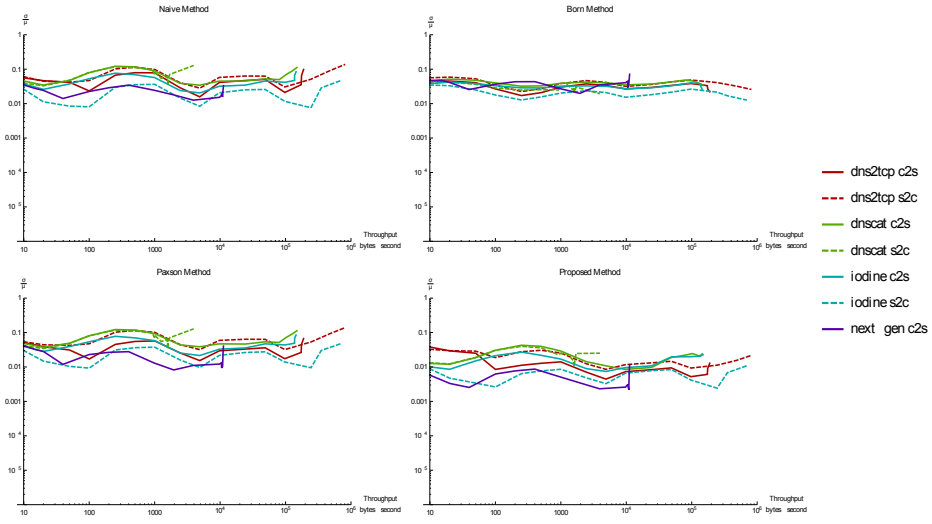


Fig. 7. Relative Standard Deviation of Metrics - All Metrics

Because of the extremely tight distributions and the insensitivity on input data distribution (described in Sect. 6), the mean value will be taken as representative of the tunnel metric for a given throughput, direction, detection method, and tunnel application. This choice of a single representative value simplifies discussion and makes presentation of the salient characteristics of the detection methods more straight forward.

Figure 8 shows several log-log plots (in order to be able to provide adequate resolution for both very small and very large throughputs), one for each detection method, that demonstrates how the mean metric generated by the methods scale as the throughput of the tunnel is increased. As is visible in Fig. 8, tunnels with lower throughput produce categorically smaller (or in the case of Born's approach, larger) metrics. This property of the lower throughput tunnels makes them necessarily harder to detect when laid over top of normal traffic. Because of this, the meth-

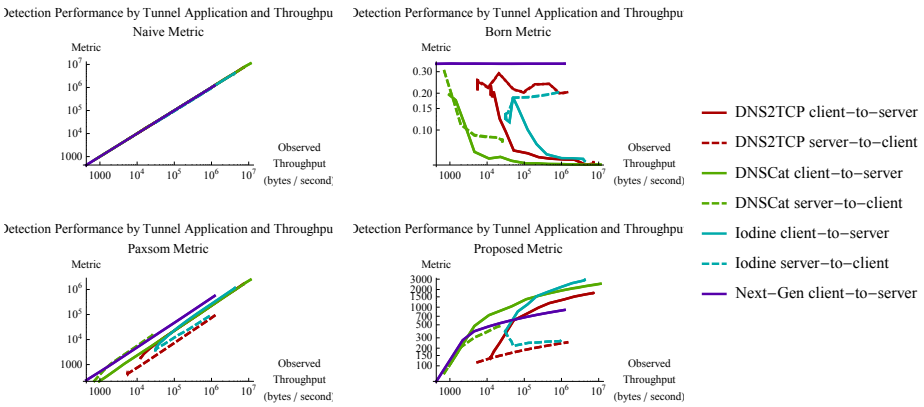


Fig. 8. These plots show how the metrics computed by the various detection methods scale per tunnelling application as a function of the tunnel throughput rates. Note that since not all tunnels are capable of a full range of throughputs (some generate a minimum amount of traffic, regardless of how low the throughput is), resulting in some of the shorter plots.

ods will be tested on their ability to detect the most hidden tunnel of each application, which in practice is one of the tunnels that transmits only ten bytes per second, against background normal DNS traffic. By testing the methods to ensure they detect low-rate tunnels, their ability to detect high-rate tunnels is implicitly demonstrated.
It is instructive to observe the relative standard deviations for the various tunnel applications and detection methods at the lowest throughput level, ten bytes per second. This is given in Table 1.

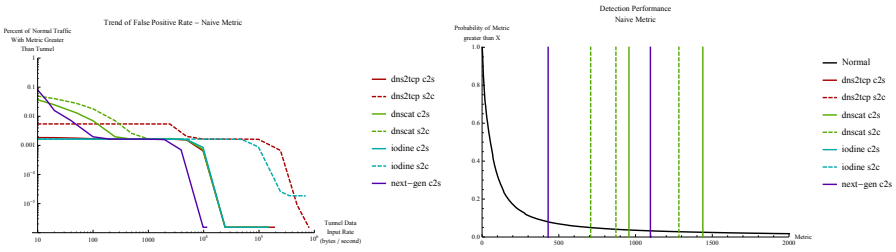
	Naive	Born	Paxson	Proposed
DNS2TCP c2s	0.056	0.050	0.045	0.037
DNS2TCP s2c	0.048	0.068	0.050	0.039
DNSCat c2s	0.016	0.053	0.019	0.0098
DNSCat s2c	0.015	0.045	0.017	0.010
Iodine c2s	0.0072	0.044	0.011	0.0050
Iodine s2c	0.0069	0.038	0.012	0.0038
Next-Gen	0.031	0.058	0.040	0.0041

Table 1. The relative standard deviation given by $\frac{\sigma}{\mu}$ of the multiple samples for each tunnel application and detection method pairing for the lowest throughput rate.

7.1 Detection Performance Against Real World Data

Since tunnel metrics are represented by a single value, the mean of their samples for a given scenario, the detection methods will be ranked based

on how they partition the metrics produced by real world data. For simplicity a thresholding approach will be considered as the classification mechanism, with anything below the tunnel's metric classified as legitimate, and anything above the tunnel's metric classified as a tunnel. Detection methods will be scored based on the number of false positives that could be expected to occur given the distribution obtained for normal traffic. The ordering is reversed for Born's method.
For each detection method, two plots are given that show how the tunnel applications compare to real world data. The first plot demonstrates how the estimated false-positive rate behaves as a function of throughput rate, direction, and tunnel application. The second plot shows the distribution of metrics of real world data with indicators represented by vertical coloured bars placed to mark the mean metrics of various tunnel application and direction pairs as given in the corresponding legend. For each marker, the false-positive rate is the y value of the normal traffic curve at intersection of the normal curve with the vertical marker. The second plot only shows the tunnelling combinations that produce the highest false-positive rates, since those are the scenarios of greatest interest. These eight plots are shown in Fig. 9 to Fig. 12.



(a) Trend of False Positive Rate for Tunnels by Throughput - Naive Metric

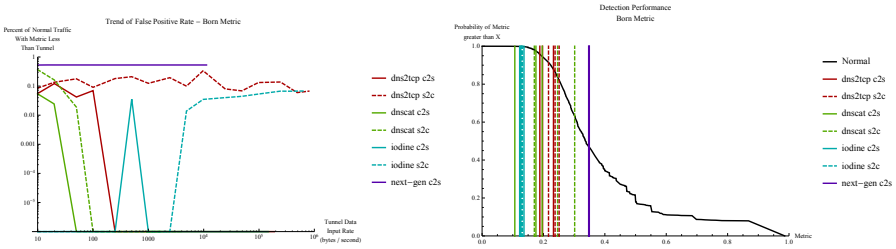
(b) Tunnel Detection Performance - Naive Metric

Fig. 9. Tunnel detection performance for the naive approach.

The naive method, due to the nature of the the capture involving (relatively) very few duplicate queries, performs quite well overall even on the next-gen tunnel traffic. Figure 9(a) shows the trends of the false positive rate for the tunnelling applications as a function of the data throughput. The lack of duplication in the DNS queries and its impacts were discussed in section 5.1 in greater detail.

7.2 Specificity and Ambiguity of Tunnel Classification

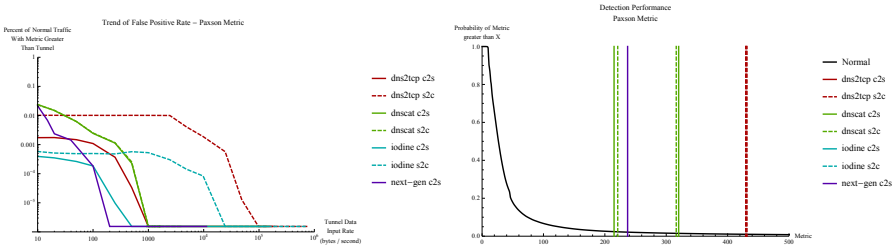
It is possible to simplify the above plots and figures into a single chart that plots the minimum detection specificity observed for each method and each tunnelling application. The following charts only consider the certainty of detecting the tunnel in which the method is least certain. By



(a) Trend of False Positive Rate for Tunnels by Throughput - Born's Metric

(b) Tunnel Detection Performance - Born's Metric

Fig. 10. Tunnel detection performance for Born's approach.



(a) Trend of False Positive Rate for Tunnels by Throughput - Paxson's Metric

(b) Tunnel Detection Performance - Paxson's Metric

Fig. 11. Tunnel detection performance for Paxson's approach.

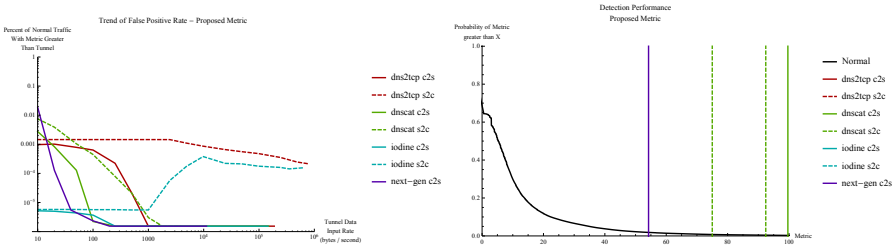
comparing the methods in their most hostile scenarios more substantial distinctions can be observed with clearer separation between the best two methods.

Figure 13(b) shows the same data as in Fig. 13(a) with a restricted range spanning the interval $[0.80, 1.00]$ as opposed to $[0, 1]$. This restricted charting range makes the the differences between the top performing methods more easily visible.

The differences between Paxson's method and our method are visible, but an additional chart further accentuating them is instructive and is shown in figure 14. In this final chart which shows a range of certainties in the interval $[0.95, 1.00]$, the differences between the two methods are clearly visible, with our approach achieving a higher certainty in every detection scenario.

7.3 Tunnel Detection Performance Conclusion

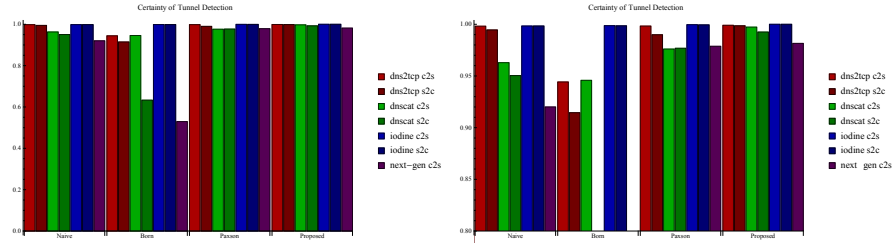
It is visible from the detailed plots in Sect. 7.1 and 7.2 that our method is superior to its peers in its ability to detect tunnels with certainty in excess of ninety eight percent. This extremely high detection rate is achieved within a very short time scale and with very low tunnel throughput.



(a) Trend of False Positive Rate for Tunnels by Throughput - Proposed Metric

(b) Tunnel Detection Performance - Proposed Metric

Fig. 12. Tunnel detection performance for our approach.



(a) Certainty of detection

(b) Certainty of detection - 0.80 to 1.00

Fig. 13. Certainty of tunnel detection by detection method.

8 Conclusion and Future Work

This paper describes our entropy-based detection method for DNS tunnels and shows through an empirical evaluation that our approach provides better detection accuracy and faster processing than previous approaches described in the literature. Our method works well not only in artificial benchmark datasets, but also in difficult real-world traffic.
Future work includes implementing our method for Bro, Snort, Suricata or other existing intrusion detection systems in order to improve the ability of organizations to observe DNS tunnels in their network. Partnership with, and adoption by, an existing industry partner would aid in the spread and deployment of this technique in enterprise and corporate environments.

References

1. K. Born. Browser-Based Covert Data Exfiltration. *CoRR*, abs/1004.4357, 2010.
2. K. Born. PSUDP — Kenton Born. http://www.kentonborn.com/psudp, jul 2010. PSUDP source code and implementation.

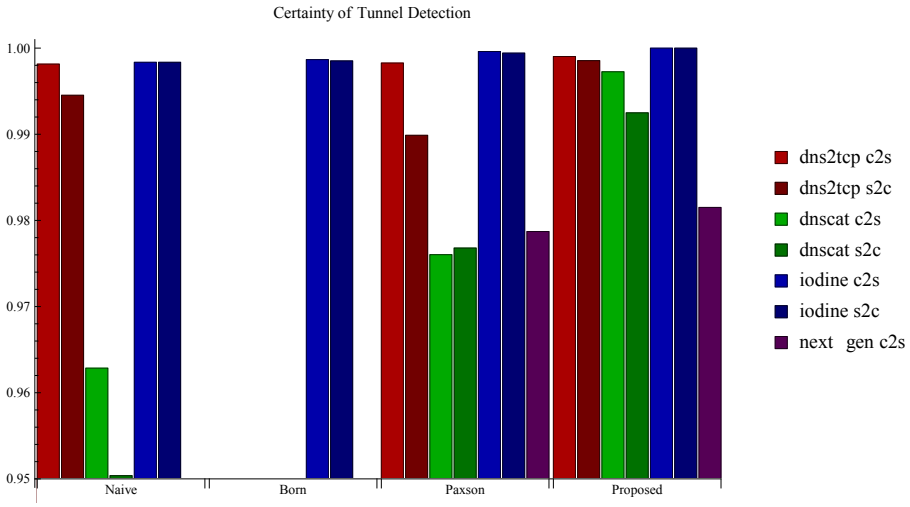


Fig. 14. Comparison of the specificity of classification of a tunnel against real-world traffic for the least certain tunnel in each detection scenario (method/application pair).

3. K. Born. PSUDP: A Passive Approach to Network-Wide Covert Communication. 2010.
4. K. Born and D. Gustafson. Detecting DNS Tunnels Using Character Frequency Analysis. *CoRR*, abs/1004.4358, 2010.
5. K. Born and D. Gustafson. NgViz: Detecting DNS Tunnels through N-Gram Visualization and Quantitative Analysis. *CoRR*, abs/1004.4359, 2010.
6. P. Butler, K. Xu, and D. D. Yao. Quantitatively Analyzing Stealthy Communication Channels. In J. Lopez and G. Tsudik, editors, *ACNS*, volume 6715 of *Lecture Notes in Computer Science*, pages 238–254, 2011.
7. M. Chamberland. Snort rules for Iodine Covert DNS Tunnel Detection. http://www.securitywire.com/2009/07/snort-rules-for-iodine-covert-dns-tunnel-detection, jul 2009.
8. H. S. Consultants. HSC - Tools - Dns2tcp. http://hsc.fr/ressources/outils/dns2tcp/index.html.en, may 2012.
9. Dennis Arturo Ludeña Romaña and Yasuo Musashi. Entropy Based Analysis of DNS Query Traffic in the Campus Network. 2007.
10. L. P. Deutsch. kryo.se: iodine (IP-over-DNS, IPv4 over DNS tunnel). http://code.kryo.se/iodine, feb 2010.
11. C. J. Dietrich, C. Rossow, F. C. Freiling, H. Bos, M. v. Steen, and N. Pohlmann. On Botnets That Use DNS for Command and Control. In *Proceedings of the 2011 Seventh European Conference on Computer Network Defense*, EC2ND '11, pages 9–16, Washington, DC, USA, 2011. IEEE Computer Society.
12. M. Dornseif. mdornseif/DeNiSe GitHub. https://github.com/mdornseif/DeNiSe, jan 2006.

13. G. Farnham. Detecting DNS Tunneling. *InfoSec Reading Room*, February 2013.
14. Internet Storm Centre - SANS Institute. Hash Database — SANS Internet Storm Center; Cooperative Network Security Community - Internet Security. https://isc.sans.edu/tools/hashsearch.html#dns_interface, oct 2013.
15. jhind. Catching DNS tunnels with A.I. http://www.meanypants.com/meanypants, jul 2009.
16. A. Karasaridis, K. S. Meier-Hellstern, and D. A. Hoeflin. Detection of DNS Anomalies using Flow Data Analysis. In *GLOBECOM*. IEEE, 2006.
17. V. Paxson. Behavioral Detection of Stealthy Intruders. https://seclab.cs.ucsb.edu/academic/projects/projects/cybaware/2011, sep 2011.
18. T. Pietraszek. DNScat. http://tadek.pietraszek.org/projects/DNScat, sep 2005.
19. J. Plenz. DNStunnel.de - free DNS tunneling service. http://dnstunnel.de, jun 2011.
20. Proventia. Proventia Server IPS - DNS tunnel traffic detected. http://www.iss.net/security_center/reference/vuln/DNS_Tunnel_Detected.htm, jan 2013.
21. S. Roolvink. Detecting attacks involving DNS servers. December 2008.
22. S. H. Sellke, C.-C. Wang, S. Bagchi, and N. Shroff. Tcp/ip timing channels: Theory to implementation. In *INFOCOM 2009, IEEE*, pages 2204–2212. IEEE, 2009.
23. P. Team. PyPy Status Blog: PyPy is faster than C, again: string formatting. http://morepypy.blogspot.com/2011/08/pypy-is-faster-than-c-again-string.html, oct 2013.
24. B. Thomas, B. E. Mullins, G. L. Peterson, and R. F. Mills. An FPGA System for Detecting Malicious DNS Network Traffic. In G. L. Peterson and S. Shenoi, editors, *IFIP Int. Conf. Digital Forensics*, volume 361 of *IFIP Advances in Information and Communication Technology*, pages 195–207. Springer, 2011.