MPTCP Robustness Against Large-Scale Man-in-the-Middle Attacks

Chi-Dung Phung, Benevid Felix Silva, Michele Nogueira, Stefano Secci

MPTCP Robustness Against Large-Scale Man-in-the-Middle Attacks

Chi-Dung Phung[a,b], Benevid Felix Silva[c], Michele Nogueira[c], Stefano Secci[a]

[a] *Cnam, Cedric, Paris, France*
[b] *Orange Labs, Chatillon, France*
[c] *Federal University of Paraná, Paraná, Brazil*

Abstract

Multipath communications at the Internet scale have been a myth for a long time, with no actual protocol being deployed at large scale. Recently, the Multipath Transmission Control Protocol (MPTCP) extension was standardized and is undergoing rapid adoption in many different use-cases, from mobile to fixed access networks, from data-centers to core networks. Among its major benefits – i.e., reliability thanks to backup path rerouting, throughput increase thanks to link aggregation, and confidentiality being more difficult to intercept a full connection – the latter has attracted lower attention. How effective would be to use MPTCP, or an equivalent multipath transport layer protocol, to exploit multiple Internet-scale paths and decrease the probability of Man-in-the-Middle (MITM) attacks is a question which we try to answer. By analyzing the Autonomous System (AS) level graph, we identify which countries and regions show a higher level of robustness against MITM AS-level attacks, for example due to core cable tapping or route hijacking practices.[1]

Keywords: MPTCP, Man-in-the-Middle attacks, communication robustness

1. Introduction

The Multipath Transmission Control Protocol (MPTCP) [24] is an extension of TCP to concurrently use multiple network paths for a given connection. Among many proposals to support these features at the transport

[1] A preliminary version of the content of this paper was presented in [43].

layer, it is considered as the one having attracted the largest interest and deployment [44]. One of the main reasons for this success is the incremental deployability adopted in its design, with the required signaling transparently reusing existing features of the TCP options.

MPTCP employs multiple 'subflows' to route traffic from a source to a destination in an IP network via different network interfaces and/or TCP ports at the transmitting and/or receiving endpoints. Subflow IP traffic can then be routed independently in the network segment. However, besides the usage of multiple network interfaces at the source or destination, the presence of flow-level load-balancers sensible to port numbers, or multipath proxies aware of the network topology [8] can differentiate the route followed by the subflow packets.

MPTCP is being adopted by major operating systems; it is already happening for Apple OSX and IOS, where it is used for some applications. Its integration in the mainstream Linux kernel is expected for the upcoming versions [48]. Among the motivations pushed forward in support of MPTCP, there are [40]: (i) bandwidth aggregation, i.e., the increased network bandwidth offered to a connection; (ii) connection reliability, i.e., the possibility to use an alternative path in case of failure along the primary path or at the primary network interface level; (iii) communication confidentiality, i.e., the decreased ability for a Man-in-the-Middle (MITM) attacker to intercept all the traffic of a same connection.

While the first two aspects above have been largely explored in the last decade, the latter was marginally studied to date. In this paper, we report the results of an extensive measurement campaign aimed at assessing the degree of confidentiality one can expect using MPTCP. In particular, we focus on confidentiality from large-scale, i.e., Autonomous System (AS) level, MITM interception, i.e., looking at the empirical probability that a single connection can be intercepted by an organization or an attacker able to capture all the traffic going through an AS on a given direction (most of Internet communications being asymmetric). Such attacks can happen either by remote access to routing devices of an AS or even by Border Gateway Protocol (BGP) route hijacking. In our analysis, we focus on the case of MPTCP-capable source devices using two edge providers, analyzing measurement results on a geographical basis to identify which countries and regions MPTCP may grant higher confidentiality with respect to large-scale MITM threats.

An important assumption of our analysis is that the MPTCP scheduler behavior of endpoints or multipath converters can be tuned so that it does

not only look for throughput maximization, but also for path diversity exploitation for increased confidentiality, as investigated in [17]. Solutions offering programmability of the MPTCP scheduler are making surface, as notably [25, 16].

It is worth noting that, despite we refer to MPTCP as our reference multipath transport-layer protocol, our study can apply as well to other functionally equivalent protocols, such as for instance multipath QUIC (Quick User Datagram Protocol Internet Connections) [14].

The paper is organized as follows. Section 2 gives a background on MPTCP and related security concerns. In Section 3, we describe our measurement methodology. Section 4 presents the results, different application scopes of this work are discussed in Section 5, and in Section 6 we conclude the paper.

2. Background

In this section we provide the necessary background on the MultiPath TCP (MPTCP) protocol and on Internet-scale Man-In-The-Middle (MITM) attacks.

2.1. MultiPath TCP (MPTCP)

MPTCP extends TCP and allows fragmenting a data flow from a single connection into multiple paths (subflows TCP) [24, 46], as illustrated in Figure 1. At the application layer, a connection appears as a normal TCP connection. At the network layer, each subflow looks like a regular TCP flow whose segments carry in their header a new type of TCP option [24]. The protocol improves the performance offered by a single flow and makes the connection more reliable using concurrent and redundant paths.

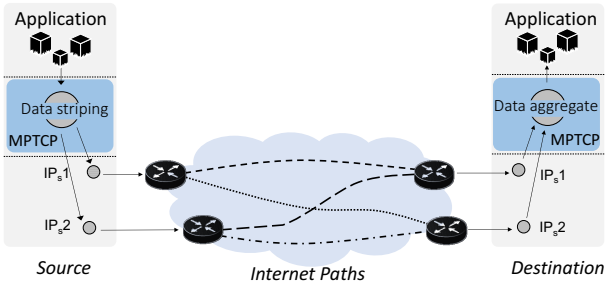


Figure 1: Multipath TCP Connection: Overview

The initial TCP connection handshake carries an option, the MP_CAPABLE option, to enable MPTCP capability discovery and subflow creation. The handshake can carry additional information, such as a cryptographic key employed to authenticate the end-hosts and set up new subflows [24]. The establishment of additional subflow may employ also a token and random numbers (nonces), to prevent replay attacks on the authentication method. Further, an additional address identifier may be employed to identify the source IP address of a packet. Hence, even if the IP header has been changed by a middlebox (e.g. NATs, firewalls), end-hosts can identify an address without any doubt or ambiguity.

MPTCP can overcome some weaknesses inherent to TCP, achieving (i) a *greater throughput*, (ii) *higher reliability*, and (iii) *higher confidentiality*. Indeed, a multipath connection can improve the throughput aggregating bandwidth over different paths by concurrent data transmission across all available paths. Moreover, a multipath connection can quickly overcome one path failure by sending data to another available path, increasing the data delivery reliability [47]. Finally, fragmenting data flow across different subflows makes complete connection interception difficult because attackers would need to capture the transmitted content through all the subflows to build the content.

Therefore, MPTCP can provide a greater level of confidentiality than a regular TCP transmission if the subflows of a connection are routed along disjoint paths: the higher the level of disjointedness, the higher the confidentiality guarantee, and furthermore the higher the level of robustness against such attacks. The goal of this paper is to precisely quantify the level of robustness in use-cases where MPTCP is adopted not (only) to improve communication performance or reliability, but (also) to improve confidentiality. When addressing this aspect, router-level path disjointedness can be considered as being too weak in particular against AS-level traffic capturing and route hijacking. This is the reason why we focus instead on a larger scale of path disjointness, i.e., AS-level path disjointedness, which do make sense in practical scenarios as elaborated here after. Running an analysis on an even larger scale than AS-level scale (e.g., regional or country level) would likely be either infeasible or not sufficiently realistic.

2.2. Internet MITM Attacks

In Internet-scale communications, MITM attacks can happen when the attacker gains access to all the traffic transiting through an AS, or at least a

portion of it that is enough to reconstruct the transmitted data. In practice, it can be possible by optical layer or BGP route hijacking MITM attacks.

At the optical layer, an attacker is able to split cables by using fiber optical taps, as described in [58], with a low probability of being detected if peculiar strategies are adopted as explained in [27, 52]. Moreover, one can intercept the traffic by exploiting coupling and out-of-the-fiber light propagation phenomena [57], despite the fact that this is particularly challenging when performing wavelength-division-multiplexing.

At the BGP layer, MITM attacks exploit the natural way BGP works, stealthily hijacking Internet routes to modify or capture the traffic before it reaches the destination. BGP-based MITM attacks have been quite deeply studied for about twenty years; in a recent survey [15] we have a detailed description of such attacks, their effects as well as mitigation and defense strategies.

This type of attack gained special attention in 2008, when a major provider in central Asia hijacked Youtube traffic to apply local policies. In the same year, a practical BGP MITM attack was demonstrated during the DefCon hacking conference [3]: authors successfully intercepted traffic bound for the conference network and redirected it to a system they controlled before routing it back to DefCon. A recent notable attack happened in 2014, attackers injected BGP routes to redirect traffic from Bitcoin miner nodes to a compromised host [30]; it was estimated that at least $83,000 worth of Bitcoins, Dogecoins, HoboNickels, and Worldcoins were stolen over a period of four months. More recently, in 2017 all traffic heading to Visa, MasterCard and other service providers was hijacked for a short period of few minutes [54]. The cost of such BGP incidents could be even more than what have been reported. Notable ones are documented in [29, 51]; often they are not reported because they cannot be always detectable, they have limited scope, last for a short time etc.

At the transport layer, the advent of MPTCP raised new security specification questions and challenges [5, 6]. In [36], cryptography based solutions are proposed against eavesdropping. The authors in [6] present an analysis of residual threats in the MPTCP signaling and propose some fixes. Recently, an extension of MPTCP to secure multipath communications was proposed in [33], to offer authentication and encryption mechanisms not only to the connection but also to single TCP options. This prevents different types of MITM attacks where an attacker could force all the traffic to be sent only over the path under his control by hijacking the traffic and erasing the

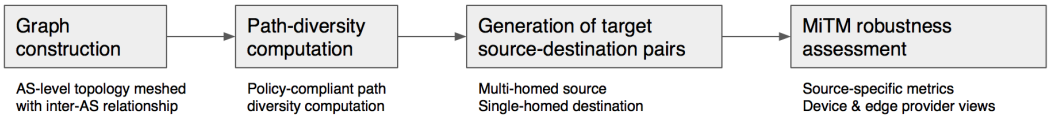


Figure 2: Adopted measurement methodology

MP_CAPABLE option.

In general, most of the works at the state of the art aim at either investigating security threats for MPTCP or proposing solutions for them. It is worth mentioning the rising interest in using MPTCP to further enhance confidentiality when using Internet over-the-top Virtual Private Networks (VPN) services such as ToR and OnionCat [31]: MPTCP is used in the upstream direction from the client to many gateways accessible via the VPN, on the way to the server, thus increasing the confidentiality level of the connection. Nevertheless, such practices can have a gain which can be hard to assess: how can you ensure the upstream source-destination traffic does follow disjoint paths, hence decreasing MITM efficiency, if not at the router-level, at the AS level? In this paper, for the first time at the state of the art to the best of our knowledge, and going beyond the preliminary study presented in [43], we attempt to provide a response to such questions.

3. Methodology

In this section, we first give a description on the datasets used for constructing a representative AS-level graph of Internet, the basis for our analysis. Then, we describe our approach for computing the number of valid vertex-disjoint paths between two arbitrary nodes over the constructed graph. Finally, we detail how we evaluate path diversity at different geographical scopes. The datasets we employed as well as our scripts are given in [41] for the sake of reproducibility. Figure 2 gives a schematic illustration of the different blocks of our measurement methodology.

It is worth noting that our methodologies imply that there is a way for a single MPTCP connection to have access to the network path diversity, by means of ad-hoc signaling or specific APIs. Solutions exist in this direction, as described in [35, 18].

3.1. Graph construction

We extract 2015 AS-level BGP-derived routing data from [4], and couple it with the inter-AS relationship data [4] (i.e., indicating which AS is provider, client or peer in an inter-AS link)[2]. The result is a new dataset containing all the AS links along with their frequency of occurrence and relationship type.

We choose this approach because, comparing with other resources [12] [32], the topological data from [4] revealed to be more reliable and able to capture a broadened view of the Internet topology. Indeed, it integrates data not only from Routeviews [50], but also from other resources such as RIPE RIS [49]. It is worth noting that the alternative traceroute-based approach employed in [12] has known issues [45] when converting router-level paths into AS-level.

Employing measurements over a long period allows us to capture inter-domain connection dynamics as well as inter-AS economic relationships. For instance, in a one month period, only 85% of inter-AS links appear more than 20 days, the remaining links with lower frequency of occurrence being those used for backup operations or during BGP convergence periods. For the sake of consistency, we removed these unstable links.

3.2. Path diversity computation

In order to have a measure of the path diversity, we need to enumerate all the paths connecting two nodes over a graph that satisfy given routing properties. This problem is often referred to as policy-compliant path diversity computation in the literature [23, 37]. The common approach [23] to this problem is to convert the original graph into a type-of-relationship (ToR) graph [21], i.e., a directed graph in which (i) the relationship between two adjacent vertexes is expressed via the direction of the edge connecting them, then (ii) maximizing the total number of vertex-disjoint paths between nodes in this graph. However, the time-complexity experienced in such methods is relatively high hence intractable for a graph as big as the AS graph.

In order to better scale, we introduce a novel path search algorithm leveraging the scale-free characteristics [2] of the input AS graph (i.e., a graph with relatively few hubs capturing the majority of the paths) to optimize the

[2]The inter-AS relationship data from [4] is extracted monthly from the Cyclops database [20], which combines BGP data with Internet eXchange Point (IXP) data and adopts inference techniques proposed in [45].

execution time. In such a scale-free graph, the diameter (i.e., the length of the longest path among all the shortest paths) is not too high. Thus, the average path length (measured in number of AS hops) connecting any pair of nodes in the AS-level graph of Internet is around 5 as of today [38] (note that it is a bit lower with IPv6).

Searching for paths in a scale-free graph, i.e., a graph with a large minority of hub nodes connecting the rest of the nodes, is a problem of controllable complexity when adopting breadth or depth-first search algorithms with a limited depth; indeed, fixing a limited depth to a graph search, and that for a scale-free graph that has a limited diameter, strongly decreases the number of explored branches in the graph exploration[3]. From the constructed AS graph G, the breadth-first search algorithm we describe in Alg. 1 can be applied to discover all the policy-compliant paths between two nodes s and d, in a reasonable time.

Alg. 1 works as follows: (i) starting from the origin s, the algorithm explores every adjacent node n of s. (ii) A queue P is introduced to keep track of the explored paths; initially, it includes all the paths from s to n. (iii) Following these paths, the algorithm continues discovering the adjacent nodes to look for destination d. (iv) For a path p dequeued from P, the last node n is extracted, all of its neighbors are checked in sequence to determine the valid next hops towards d. (v) Once a neighbor is determined as valid, link to that neighbor will be added into the current path forming a new valid path toward destination. This new explored path is then enqueued into P for the next discovering phase. (vi) A node is considered as valid once the path through it does not violate the valley-free routing property [28][4]; we express such policy-compliant path (i.e., a path that complies with the valley-free routing policy), using the following regular expression $c2p * p2p?p2c*$ [37] in which $c2p$, $p2p$ and $p2c$ denote the relationship between interconnected nodes (where ? means that you can have one or none p2p link).

[3]breadth-first search explore first all the neighbors of a node, and then explore deeper in the graph; depth-first search, instead, explore first in depth starting from a given neigbor, and proceeds to the next neighbour only when the exploration in depth from the first one has terminated.

[4]A valley-free path is defined as a path that does not cross more than one peering agreements, which are agreements over which two ASes exchange only routes towards respective customers, which is justified by the fact that peering agreement are meant to be free-of-charge for both ASes

It is worth noting that, within G links are labeled according to their inferred relationship. For example, assuming that n_1, n_2, n_3 are neighbors of node s, in which s is customer ('c') of n_1, provider ('p') of n_2 and peer with n_3; the links (s, n_1), (s, n_2), and (s, n_3) are labeled as '$c2p$', '$p2c$' and '$p2p$', respectively. With these labels, the regular expression for policy-compliant path then could be leveraged to determine the validity of next hop toward the destination. For instance, taking the customer-type neighbors among the neighbors of s (i.e., n_2), and looking at their neighbors x in turn, those (n_2, x) links are not validated if they are either $c2p$ or $p2p$ because a customer is not expected to grant transit towards its other provider(s) to one among its providers, and a customer is not expected to give access to its peer(s) to its provider(s). By checking the labels of links along the explored path, the validity of next hops can be determined. Once a valid path is discovered, it is enqueued into P for the next discovering phase. The same exploration and validation processes are repeated for all the paths in P until reaching destination d or the path length goes over a given threshold τ.

The path validation executes at run-time to ensure that non-compliant paths are detected at the early stage, thus avoiding wasting time exploring invalid paths. By reducing the number of paths needed to be explored in the following phases, the search space is continuously optimized. Moreover, a proper choice of τ not only limits the time and space complexity, but can also avoid selecting long paths to be avoided in practice.

As a result of the path search algorithm, policy-compliant paths between two endpoints may share common nodes. To get the final set of vertex-disjoint paths, we run a simple off-line filtering linear algorithm to capture the shortest disjoint paths. Since the original list of valid paths turned out to be quite small most of the time and already sorted, the complexity of such a filtering operation is negligible.

3.3. Source-destination pairs

Within the constructed AS-level graph, multipath connections could be simulated by simply attaching end-hosts as virtual nodes into AS nodes of the original graph. For instance, a multi-homed device can be emulated by adding a new node, then linking it with at least two AS nodes. The connection from that node to any other virtual nodes forms a multipath transport-layer communication. Our approach for emulating multipath communication can therefore be simply referred to as a process of source-destination pair selection. In the following, we define the target set of AS nodes which we

Algorithm 1: Path Search Algorithm

```
input  : source s, destination d, graph g
output: ValidPathSet
VisitedNodes ⟵ ∅
queue.append([s])
while queue not empty do
    path ⟵ queue.pop()
    v ⟵ path.LastNode()
    if v ∉ VisitedNodes then
        for n ∈ v.NeighborSet do
            if n ∉ VisitedNodes and (label(v,n)='p2c' or
            label(v,n)='p2p') then
                for x ∈ n.NeighborSet do
                    if label(n,x)='c2p' or label(n,x)='p2p' then
                        g.RemoveEdge(n,x)
                    end
                end
            end
            NewPath ⟵ list(path)
            NewPath.append(n)
            if n = d then
                ValidPathSet.append(NewPath)
            end
            if length(NewPath) = τ + 1 then break
            queue.append(NewPath)
        end
        VisitedNode.add(v)
    end
end
```

consider for attaching the end hosts. A simulation process is then described in details explaining which communication scenarios are covered in our study.

The current Internet ecosystem is composed of more than 70 thousand ASes, out of which the large majority are stub ASes, i.e., ASes that are only origin or destination ASes. About 13% are Tier-3 or small Tier-2 ASes, we arbitrary define in this paper as those appearing at most in the third from last position and at least penultimate position in BGP AS paths; we refer to such ASes as 'edge provider' ASes, which can be considered as a representative set of national Internet Service Provider (ISPs). Such ASes are often referred to as 'eyeball' ASes. In this paper, an edge provider AS is not a stub AS, but is rather expected to be a regional or national ISP, most of the time (rare are the cases where an international/intercontinental ISP gives Internet access to end-users).

Rather than taking into account all possible communications, we target the connections among hosts at the edges, performing connections using multiple sub-flows such as done with MPTCP. Considering connections between hosts in different countries, we precisely address the MITM robustness of Internet connections crossing multiple ASes. To precisely determine which communications to cover in our study, we define a target set of source-destination pairs that address, in a reasonable yet arbitrary way, the communications that may be more sensitive to communication privacy. Our choice of source-destination pairs is as follows:

- the source is interconnected to two edge providers in a country.
- the destination is not multi-homed, i.e., it is reachable via a single ISP, the one given by the best BGP path from each source edge provider, and belongs to an AS at another country than the one of the source.

Figure 3 illustrates an example of how we simulate multipath communications accordingly the above policy. For each two arbitrary edge provider ASes in a same country, one source is created (i.e., a dual-homed source). For each edge provider in another country, one destination is paired with the source. Such a pair dual-homed source - single-homed destination defines the two endpoints of a multipath communication. Listing all pairs, i.e., combining a given source with every destination, all possible (international) communications of a dual-homed host can be covered.

Besides reducing the number of pairs to a reasonable and treatable number (requiring about one week of computation), it is worth noting that, in

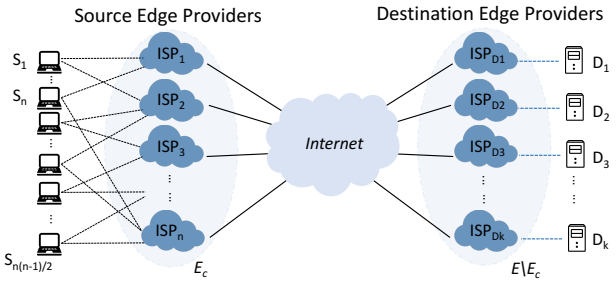


Figure 3: Representation of the source-destination pair selection process.

such a way, we consider communication in a single direction: from source to destination. That is, under such a path election strategy, we cover the case when a multi-homed device *uploads* to a single-homed server, as well as the case when a single-homed device *downloads* contents from multi-homed servers.

The scenarios that are not covered in our study include: (i) multi-homed devices *downloading* from single-homed server; (ii) single-homed devices *uploading* contents to multi-homed servers; (iii) a multi-homed device communicating with another multi-homed device. A dual analysis, quite expensive computationally, covering these additional cases may be performed as well in future works.

3.4. MiTM robustness metric aggregations

The ability to split traffic over different paths allows multipath protocol to realize MiTM attacks more difficult. Thus, the chance for an attacker to capture all the traffic sent by a source is reduced in proportion to the number of disjoint paths between the source and the destination. Path diversity is therefore a proper indicator to evaluate the MiTM robustness of a multipath communication.

Rather than considering the robustness against MiTM attacks of every connection individually, we are more interested in evaluating such a robustness at the end-host level, thus measuring the degree of robustness offered by a multipath-capable source device to secure its data sending over the Internet.

3.4.1. Source-specific MiTM robustness metric

With regard to the aforementioned approach for source-destination pair selection, we define the *source-specific MiTM robustness metric* as the aver-

age number of disjoint paths over all the destination edge providers that are in a different country than the source. Such a metric can be considered as a level of unlikelihood that a MiTM attack takes place for that source configuration; the higher the value of the robustness metric, the more difficult it is for an attacker to capture traffic from that source.

3.4.2. Source country-specific MiTM robustness metric

Aggregating results from all the sources within a given country we can obtain a *source country-specific MiTM robustness metric*. Such a definition allows us to characterize the robustness level offered by different source countries to multipath communications.

3.4.3. Country-level source-destination MiTM robustness metric

As another way to aggregate the MiTM robustness metric computation, we also study a country-level source-destination based aggregation, i.e., leading to a robustness metric for a pair of source and destination countries. Given a source (a pair of edge providers in a country) and a destination country, its MiTM robustness metric is defined as the average number of disjoint paths from the source over all edge providers belonging to the destination country.

3.4.4. Country-pair MiTM robustness metric

By grouping together the results from all the sources within a source country, we can define the *country-pair MiTM robustness metric* for the corresponding pair of countries.

3.4.5. Metric computation

Let us more precisely characterize the aforementioned source-destination pair selection process with respect to the two MiTM robustness metric aggregations we study in the following, i.e., the source country-level one and the country-pair one. We segment the set of edge providers, E, in country-specific subsets, E_c, where c denotes a country in the set of countries C, i.e., $E = \bigcup_{c \in C} E_c$. We employ the AS-to-country mapping given by the CIDR Report [7]. Let us indicate with $E_{\tilde{c}}$ the restriction to a specific country $\tilde{c} \in C$. Overall, for a given country $\tilde{c}$, the number of source-destination pairs is therefore equal to the number of pairs of edge providers for the given

country multiplied by the number of edge providers of other countries, i.e.

$$\frac{|E_{\tilde{c}}| \times (|E_{\tilde{c}}| - 1)}{2} \times \sum_{c \neq \tilde{c}} |E_c| \tag{1}$$

For a given source and destination countries, s and d respectively, the number of source-destination pairs connecting them is equal to:

$$\frac{|E_s| \times (|E_s| - 1)}{2} \times |E_d| \tag{2}$$

Doing so, we target a lower bound, pessimistic analysis, since we only take into consideration international communications and we suppose the destination is not multi-homed. The filter we set on the destination enumeration allows us to target communications that may need a higher level of confidentiality due to their international connotation. Moreover, in this way we also avoid a huge bias potentially due to the fact that a large majority of the AS paths available at the national level are not visible in backbone BGP routing tables such as the Routeviews ones (typically because of Internet exchange points, as recently shown in [1]). We believe having a lower bound stand is more appropriate than an upper bound one, while allowing us to scientifically qualify the value of the relative trends.

4. Results

We report the results obtained for a set of 147 countries, i.e., those countries from the United Nations statistics [56] that appear to have at least two distinct edge providers officially based in the country; this automatically excludes Greenland territories, very small city-state countries, many African countries and Indonesia. The geographical coverage is given in Figure 5. In the following sections, we present the statistics for two different MiTM robustness metric aggregations, the country source specific one and the country pair one.

4.1. Source country aggregation

Let us recall the measurement approach for source country-specific MiTM robustness analysis:

- For each country, we generate all possible dual-homed sources, i.e., all possible pairs of edge providers.

- For each such source configuration, we compute the number of disjoint paths to each destination. For each edge provider that is a different country than the source country, one destination is generated.

- For a given source, we compute its corresponding robustness metric by taking the average of the number of disjoint paths over all the destinations.

- For each country, a series of MITM robustness metrics is hence generated, one for each source.

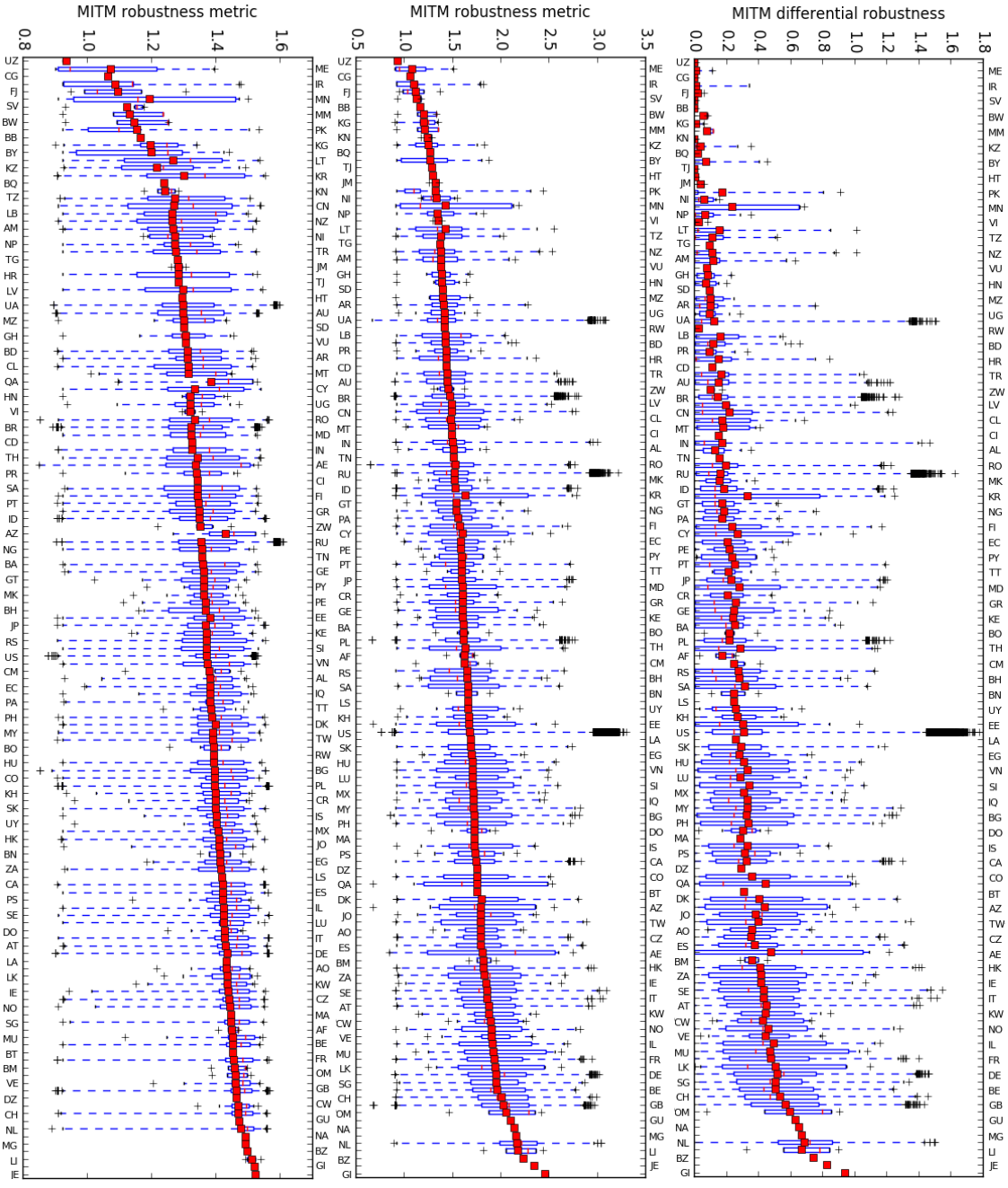
We characterize the resulting series using boxplot distributions (using a 0.1% outliers threshold). We overlay over the boxplots the average of the corresponding series with a red square, order them with increasing averages[5] from left to right. We report the results in Figure 4, and with a geographical view in Figure 5. We express three different viewpoints:

- *device view* (Figure 4a): the MITM robustness is computed with the source node integrated in the AS graph as an 'artificial' node, i.e., the path search algorithm finds the number of AS-disjoint paths from this source node toward the destination. It provides therefore a device view; obviously, in this view the upper bound of the robustness is 2, i.e., the number of edge providers used by the source.

- *edge provider view* (Figure 4b): the MITM robustness is computed counting the number of disjoint paths from the first and the second edge provider, then decreased by those paths that share an AS hop. Taking into account such a view, we assume that additional AS paths can be made available to MPTCP subflows acting at the edge providers level, e.g., by forms of flow path steering and load-balancing.

- *differential view* (Figure 4c): the differential robustness results, i.e., the edge provider view robustness minus the device view robustness, computed for each source configuration individually. This view more precisely quantifies the gain achievable for MPTCP communications when inter-AS load-balancing is enabled at the edge providers.

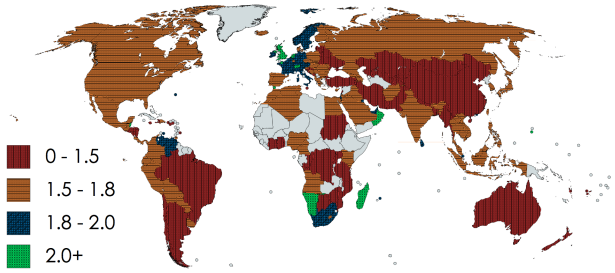
[5]Average values do include outliers.



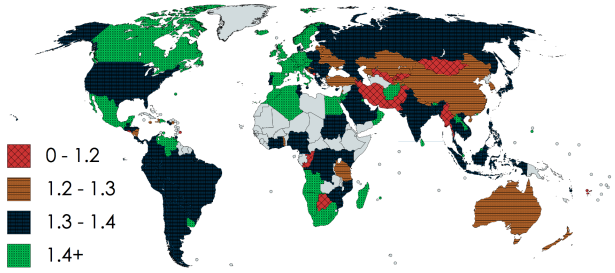
(a) device view (b) edge provider view (c) differential robustness view

Figure 4: MITM robustness distribution for 147 countries.

The above viewpoints also reflect different levels of trust on the providers. That is, while the edge provider view assumes MITM attacks do not happen at the source and destination edge providers (i.e., there is a high level of trust on those providers), the device view assumes that attacks can happen at the source edge providers, hence revealing a low level of trust in source direct providers.



(a) device view



(b) edge provider view

Figure 5: Countries covered with corresponding MiTM robustness distribution

As a general assessment, Figure 4 shows a distribution to be interpreted. For example, one could consider 1.5 as the rough threshold above which the likelihood of MiTM is to be considered low, and conversely high if lower than 1.5. Only about 5% of the countries show good chances of being robust against MITM from a device viewpoint, while looking at the maximum instead of the average and median values one could speculate that careful choice of the edge providers could make the MiTM likelihood low for a majority of the countries. From an edge provider viewpoint, this ratio grows to roughly 60%, and higher than 90% looking at the maximum, that is if the edge provider choice can be influenced by confidentiality concerns.

Moreover, the average number of paths connecting a dual-homed node to international destinations has a significant variance depending on the origin

country. The average robustness ranges from 1 (and less) to 1.6 from a device viewpoint, and from 1 (and less) to 2.5 from an edge provider viewpoint. It is worth noting that the reason why some minimum, and even average values, are below 1, is the partial view over the Internet topology and the incompleteness of inter-AS relationship inference; in fact, these factors make some destinations unreachable (counted as 0 path), but we left the 0 values in the series to also give an index of the level of topology incompleteness for different countries. In any case, the boxplot median is a metric robust against such outliers to look at.

In addition, observing the distributions in Figure 4, we can also remark that:

- Within a country, a high inter-quantile range indicates that the path diversity strongly depends on how the two upstream edge providers are selected for the source.

- The gap between the min and max robustness is another interesting fitness metric to observe. Some countries maintain a small gap (below 1) while others have a very big gap (up to 2). In other words, the deployment of multipath transport-layer communications for securing international communications in some countries can statistically yield a much better result than in other countries, where this gap is smaller. Particularly interesting is the case of Angola (AO), Venezuela (VE) and Namibia (NA), with small robustness gaps, which may be correlated to the presence of inter-continental cables landing in or close to the country [11].

- The median is mostly higher than the average in the device view, and lower than the average in the edge provider view. This is essentially due to outliers, counted in the average and not in the median.

- From the edge provider viewpoint, the maximum value is higher than 2 in the most of the countries, suggesting that with a proper choice of trusted source providers, one can adopt multipath communications to statistically expect high confidentiality for its communications. Particularly alerting are the cases of Uzbekistan (UZ), Nepal (NP) and Lebanon (LB), with quite low maximum values.

- From the device viewpoint, in most of the cases the maximum robustness is not higher than 1.6, both averages and medians are quite far

from the desirable target of 2. Hence, without the support of inter-AS load-balancing at source providers, path diversity from a dual-homed node is reduced significantly, indicating a non negligible probability of paths joining on the way to the destination.

- Considering the differential robustness, we can remark that among the countries that have the lowest device view MITM robustness, those that could most benefit from inter-AS load-balancing practices are Mongolia (MN), Pakistan (PK) and Korea (KR). However, the majority of those countries with low robustness do not improve much the situation going from the device view to the edge provider view.

Looking at macro geographical regions, many European countries seem to grant better security than countries in other regions. In order to look at continental characteristics, the plots in Figure 6 show the boxplot results (with 1% outliers) aggregated on a macro-region basis (a and c, sub-continental level) and on a relative position basis (b and d, in terms of seacoast and inland borders). We can remark that:

- Western Europe appears to be the best off, followed by Northern Europe and Northern America. In almost 50% of Western Europe countries there can be 2 disjoint paths from the source edge providers to Internet destinations.

- Central Asia shows the worst robustness, followed by Australia and New Zealand; the reasons are likely network centralization practices and geographical isolation. It is interesting to notice the relevant gap between Central and South-Eastern/Western Asia.

- within Europe, Western countries do offer a better diversity over Northern countries, and especially over Eastern and Southern countries. with a small range of variation and a high median value show the best result.

- A high variance is recorded at Southern Asia, Northern Europe and Sub-Saharan Africa, which indicates high differences among the countries within these areas.

- We could not find a strong correlation between the relative continental position, and the robustness metric, yet a positive correlation exists, with countries at the boundaries of oceans, with inter-continental cable

landing and that are sea-oriented (most of the border on the coast) that offer higher robustness than fully internal and continental-oriented ones.

4.2. Source-destination country pair aggregation

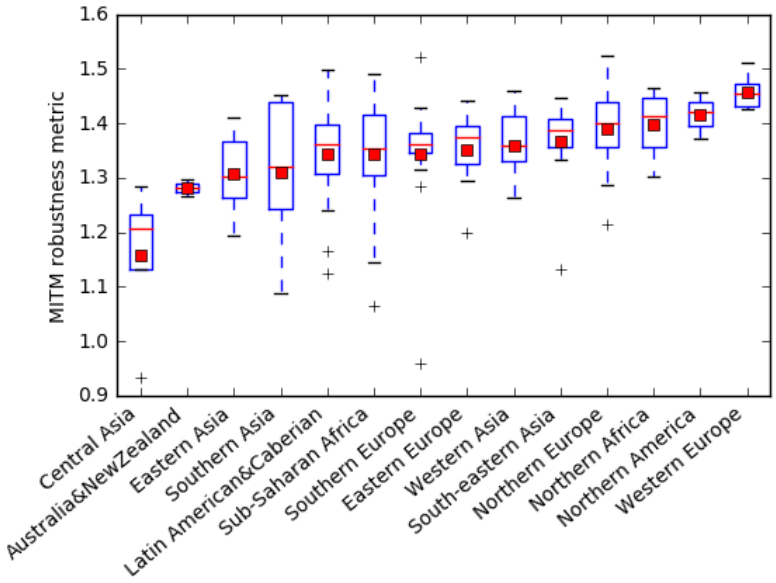
As we may notice, the MiTM robustness level of a multipath communication could be affected not only by the country where the communication starts but also by the choice of upstream providers at that country. Besides that, within a source country, the robustness level for different destination countries can significantly vary. To evaluate this latter aspect further, we perform a source-destination country pair aggregation.

Over the set of 147 countries, we evaluate the robustness metric for 1547 directional country-to-country communication pairs in which the MiTM robustness metric for one pair is computed as follows:

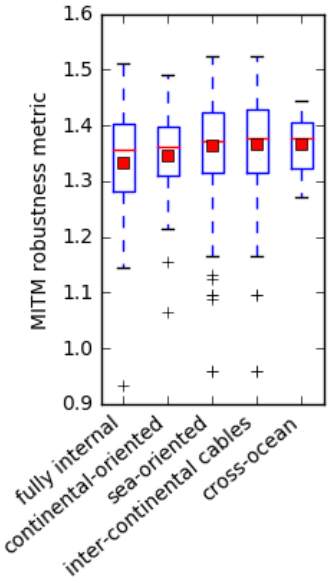
- For a given source country, we generate all possible dual-homed sources, i.e., all possible pairs of edge providers.
- For each such source configuration, we compute the number of disjoint paths to each edge providers located in the destination country.
- For a given source, we take the average of the number of disjoint paths over all the destinations to get its source-destination based MiTM robustness metric.
- For a given source-destination country pair, a series of MiTM robustness metrics, one for each source, is therefore created.

In Figure 7, we report the CDF of the average MiTM robustness, for all the 1547 pairs. The high range of variation (between 0.4 and 6) shows us the big robustness gap between pairs. Only 20% of the country pairs show an average of two or higher. For the remaining pairs, approximately 73% of them have the average range from 1 to 2. The remaining 7% are country pairs with very low robustness, below one; besides the specific context related to a country pair, a factor behind such bad performance can be the already discussed topology view incompleteness.

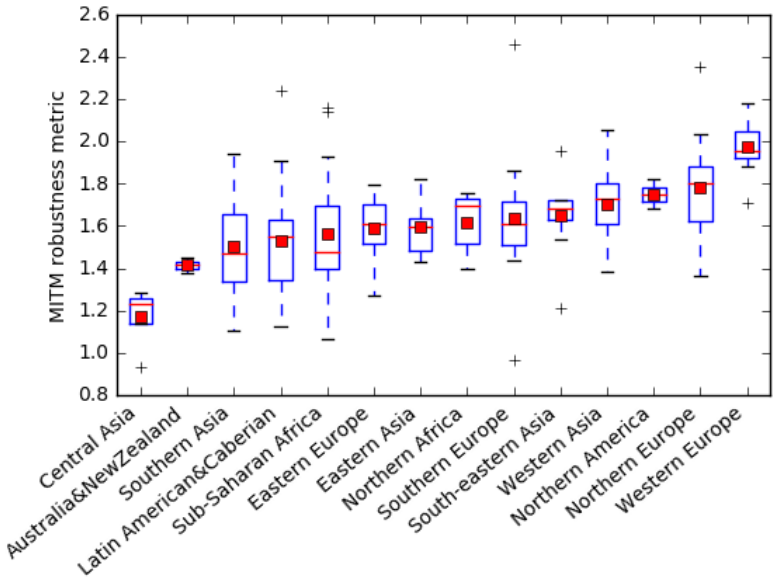
To better understand the impact caused by different destinations, we further characterize the top 147 and bottom 147 pair in the CDF distribution, i.e., roughly the top 10% and the bottom 10% cases. The results are presented



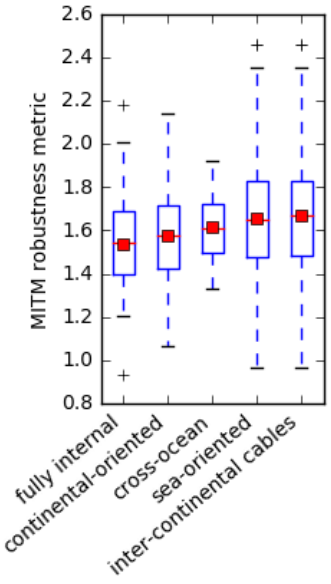
(a) device view: macro-regions grouping



(b) position grouping



(c) edge provider view: macro-regions grouping



(d) position grouping

Figure 6: MITM robustness metric with continental subregion grouping.

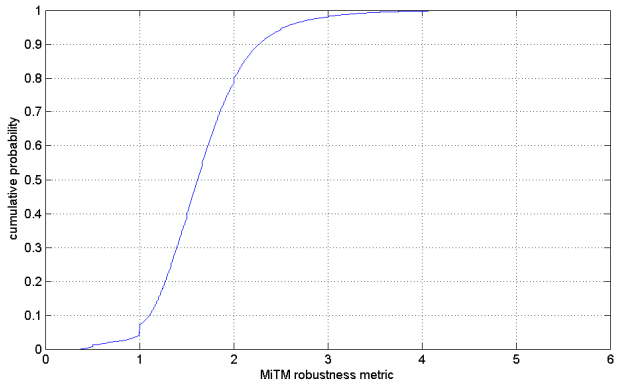
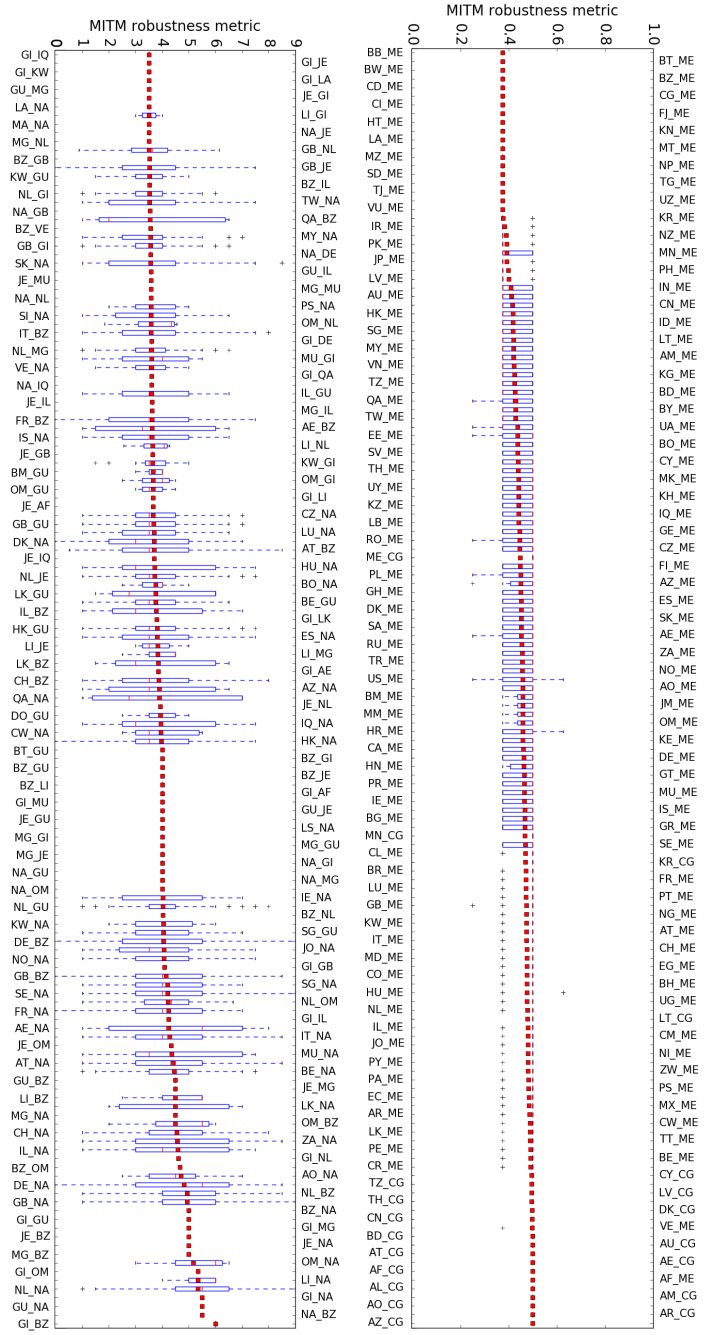


Figure 7: CDF of average MiTM robustness for 1547 pairs of source-destination country

in Figure 8, where the country pairs in each group are ordered from left to right with an increasing average (the average do include the outliers). We report the MiTM robustness distribution of each pair using the boxplot (with 0.1% outliers) overlaid with a red square representing the average.

Figure 8a reports the MiTM robustness metric distribution for the top 147 country pairs. The high inter-quartile range (IQR) with a pair highlights the strong impact caused by edge providers choice at the source to the robustness metric. Besides that, there are also some source countries, such as Morocco (MA), Madagascar (MG), Gibraltar (GI), Guam (GU), Jersey (JE), Namibia (NA), Liechtenstein (LI) and Belize (BZ), that suffer from the presence of only one edge provider pair; these countries result in pairs with a collapsed robustness point in the box. In addition, within these top 147 pairs, there are some destinations, like Namibia (NA), Guam (GU) and Belize (BZ), that appear to show high sensibility to the destination choice on the MiTM robustness.

In Figure 8b, we report the results for the bottom 147 country pairs. The majority of them have Montenegro (ME) as the destination. The second destination is Republic of Congo (CG). That highlights again the impact of destination choice on the MiTM robustness level. Unlike the top 10% case, we see a small inter quartile range (IQR) for most of the pairs, showing that even a careful choice on the edge providers at the source country cannot improve much the level of robustness for such connections. In other words, regardless of the origin country as well as the choice of source edge providers, the possibility of employing MPTCP to secure the communications destined



(a) 147 most robust country pairs

(b) 147 least robust country pairs

Figure 8: MITM robustness distribution for the top and bottom 147 pairs of country (with respect to their average MITM robustness)

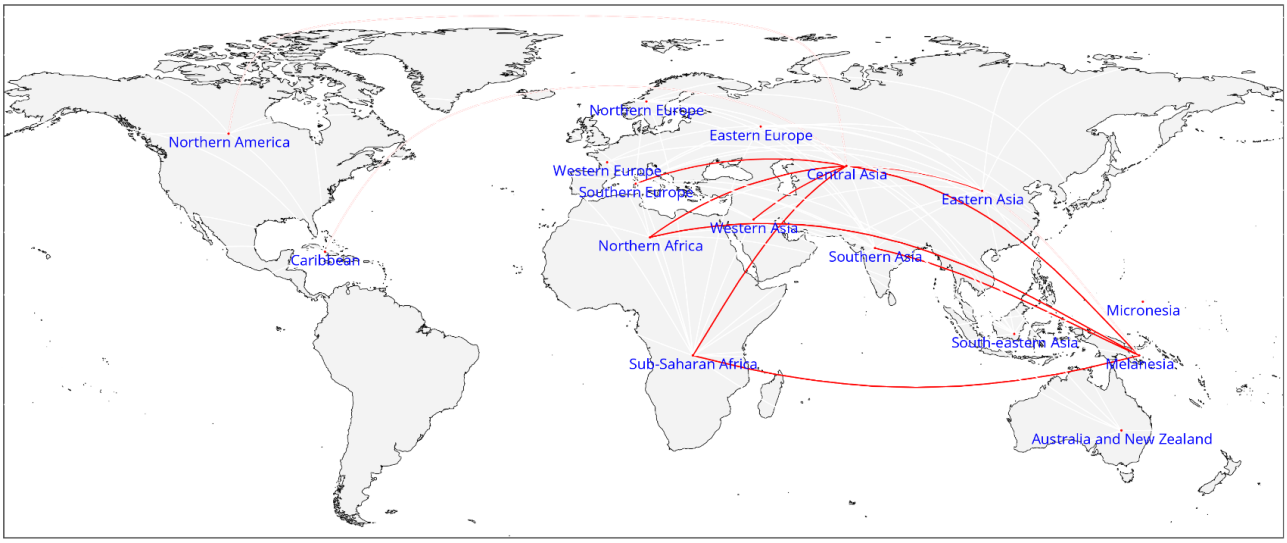
to, e.g., Montenegro and Republic of Congo is extremely low.

Considering 1 and 2 as the thresholds for very low (zero) and high (sufficient) robustness, respectively, a source-destination pair can be classified as: (1) highly robust against MiTM if it has the average robustness level of at least 2, and (2) weak against the MiTM once maintaining the average of 1 or lower.

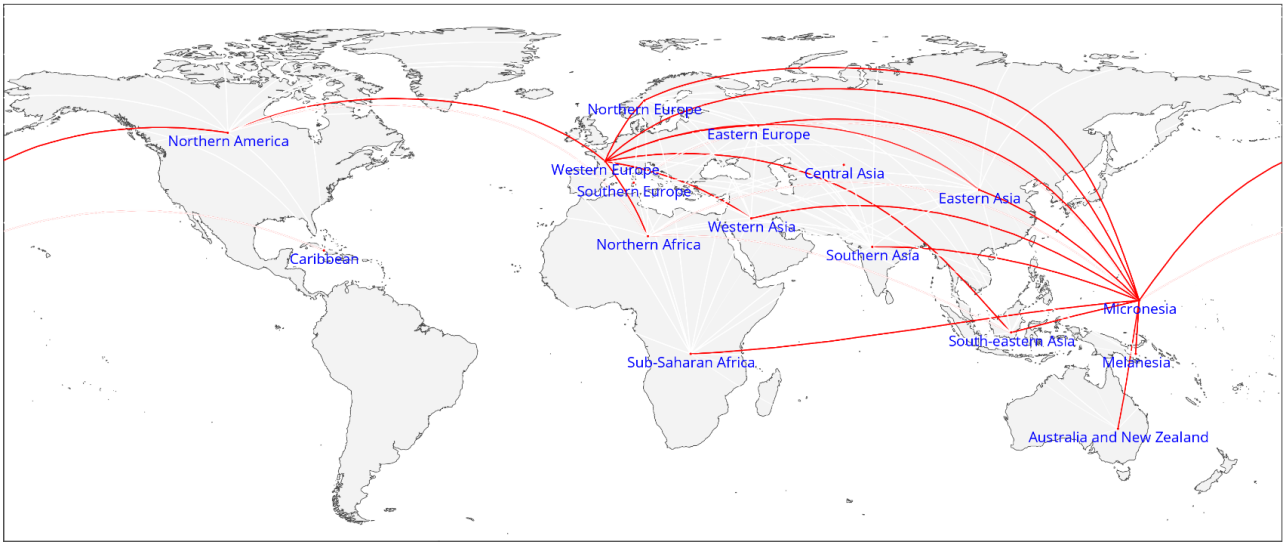
We visualize the country-to-country communications in these two classes by mapping them into a geographical map in Figure 9. To avoid too many lines, we first group countries with respect to their subregion, then converting these country-to-country connections into the corresponding subregion-to-subregion connections. Finally, the subregional connections are expressed using lines with different opacity reflecting the portion of country-to-country communications between subregions having the MiTM robustness level less than or equal to 1 as in Figure 9a, and equal to or higher than 2 as in Figure 9b.

In Figure 9a, we only show the connections between subregions when there are more than 30% of the country-to-country communications with a robustness metric of at most one. For subregion pairs with less than 30% of their country-to-country communications having a robustness metric lower than one, the connection lines are hidden. In other words, the lines point out the subregions where the deployment of MPTCP cannot offer any protection against large-scale MiTM attacks. As presented in the map, the area of Central Asia and Melanesia are the two subregions having the worst performance, most of their MPTCP communications with other subregions are classified as zero-robust. Thus, most of the subregions could not be benefit from the deployment of MPTCP to secure their communications with Central Asia.

In the sub-regional view of the high robustness group presented in Figure 9b, we show the connection lines between sub-regions with more than 50% of the country-to-country communications having robustness level of 2 or higher. In such a view, Micronesia and then Western Europe are the two areas that outperform the others in term of MiTM robustness. As depicted in the plot, except for a few low connected regions, like Central Asia, Caribbean and Northern Africa, etc., most of the multipath communications from and to Micronesia can profit from a high level of robustness. It is worth noting that in the region of Micronesia, Guam is the only country covered by our study. The high robustness result captured for communications from and to this region is therefore directly related to the highly connected network infrastructure of Guam being a crucial node in the Internet cable network [53].



(a) regions with more than 30% of country-to-country communications having at most one path



(b) regions with more than 50% of country-to-country communications having at least two paths

Figure 9: Regional view of the source-destination based MiTM robustness

5. Practical aspects

We focused our study on MPTCP-based communications. More precisely, it covers the following cases:

- *MPTCP capable endpoints*: both source and destination, client and server (or vice versa), are MPTCP capable, and the MPTCP communication is not filtered by middle-boxes. As argued in Section 3.3, the multi-homed endpoint can be either the server or the client.

- *MPTCP proxied endpoints*: at least one endpoint is not MPTCP capable, but the TCP communications are handled by MPTCP proxies, converting TCP packets into MPTCP packets and vice versa, as explained in [8, 10], possibly routed via Internet disjoint paths as proposed in [19, 9]. The multipath conversion proxies can sit at endpoint premises (customer premises equipment for the client, hypervisor or middle-box at the server) or at the edge provider level borders.

Besides MPTCP-based communications, other protocols offering Internet-scale multipath, connection flow-level load-balancing could also be covered by our study. The following protocols are either not deployed, or they have only undergone a limited deployment at the Internet scale so far; they are:

- *SCTP*: the Stream-Control-Protocol (SCTP) [55] is another multipath transport protocol absolving the same function as MPTCP, but less deployed than MPTCP due to the limited retrocompatibility.

- *LISP*: the Locator/Identifier Separation Protocol (LISP) [26] is able to perform inter-AS inbound load-balancing by means of encapsulation, routing locator mapping, and appropriate traffic engineering (TE) policy configuration. LISP primary scope is the edge provider one, hence results with the edge provider view are readily applicable. Furthermore, deployment of LISP as an intra-AS TE tool can also allow us to perform inter-AS multipath on the outbound direction as proposed in [42].

- *MultiPath BGP*: in BGP, the routing decision process only allows us to take one route per network prefix. The selected path can be inefficient in terms of global routing. Recently, forms of *Multipath BGP* were discussed in standardization fora, but finally not standardized; however,

some recommendations have been published [39], and implemented by some vendors (see, e.g., [34] and [13]). Such multipath mode can be adopted at the edge provider scope to enable load-balancing at the egress direction. Despite the study [22] on core routing tables reports that in 2010 multipath BGP was practically not used, speculations report that it is used by major cloud providers.

The above protocols are a selection of those protocol communication contexts where load-balancing can affect the AS-path selection. There are also other load-balancing protocols which can potentially influence the egress AS selection as well, as for instance in data-center environments. In the case of MPTCP communications, these protocols, operated at the edge provider view, are able to perform inter-AS load-balancing in such a way that the path diversity exposed in our edge provider view can be made available to MPTCP devices, hence giving them the full potential of MPTCP in terms of communication confidentiality and robustness against MITM attacks.

Finally, additional multipath transport-layer protocols are making surface, as for example the already mentioned multipath extension to the QUIC protocol [14], nicknamed MPQUIC. As MPTCP that authenticates its options to avoid interference from one path to the others as already discussed, MPQUIC also has a similar protection by default, because every control information in QUIC is authenticated.

6. Conclusion

We explored in this paper how Internet path diversity could be exploited by means of multipath transport-layer protocols such as MPTCP, when looking at increased security against man-in-the-middle attacks. We focused on such attacks acting at the autonomous system level, and at the robustness of multipath communications in what appear as a reasonable configuration where at least one endpoint is multi-homed with two edge providers.

We reported extensive, specific and aggregated results for most of the world countries and regions, looking at macro trends that could inspire further research in the area. Results show that, statistically speaking, a multipath protocols such as MPTCP does not help in guaranteeing robustness against MiTM attacks hence high confidentiality, unless (i) the choice of the edge provider is carefully taken, or (ii) one can rely on inter-AS load-balancing features offered implicitly or explicitly by edge providers. Some

continental regions are strongly more robust than others, and there seems to be a positive correlation with inter-continental cable landing proximity. Moreover, the results show that there are countries surprisingly less well connected than one could think of, such as Northern America countries, and countries that are more obviously less robust against such attacks due to network centralization practices.

It is worth mentioning that the methodology we propose to measure MiTM robustness could be instrumental also for other types of analysis. For instance, having a high MiTM robustness may also represent an increased sensibility to distributed denial of service attacks (DDOS), as the set of possible sources not sharing a network bottleneck can be expected to increase with the AS-level path disjointness. This aspect may be object of further work.

Acknowledgement

We acknowledge the support and relevant effort of Ho Dac Duy Nguyen in the preparation of the data processing and methodology. This work was partially funded by the French Investissement d'Avenir FED4PMR project. We thank Xenofontas Dimitropoulos for his valuable feedback.

References

[1] Ager, B., Chatzis, N., Feldmann, A., Sarrar, N., Uhlig, S., Willinger, W., 2012. Anatomy of a large european IXP. In: ACM SIGCOMM 2012 Conference, SIGCOMM '12, Helsinki, Finland - August 13 - 17, 2012. pp. 163–174.
URL http://doi.acm.org/10.1145/2342356.2342393

[2] Albert, R., Barabási, A., 2001. Statistical mechanics of complex networks. CoRR cond-mat/0106096.
URL http://arxiv.org/abs/cond-mat/0106096

[3] A.Pilosov, T.Kapela, 2017. Stealing the internet - an internet-scale man in the middle attack.
URL https://www.defcon.org/images/defcon-16/dc16-presentations/defcon-16-pilosov-kapela.pdf

[4] AS-level Topology Archive, 2015. As-level topology archive.
URL http://irl.cs.ucla.edu/topology

[5] Bagnulo, M., March 2011. Threat analysis for tcp extensions for multipath operation with multiple addresses. RFC 6181, RFC Editor.
URL https://tools.ietf.org/rfc/rfc6181.txt

[6] Bagnulo, M., Paasch, C., Gont, F., Bonaventure, O., Raiciu, C., July 2015. Analysis of residual threats and possible fixes for multipath tcp (mptcp). RFC 7430, RFC Editor.
URL https://tools.ietf.org/rfc/rfc7430.txt

[7] Bates, T., Smith, P., Huston, G., 2017. Cidr report.
URL http://www.cidr-report.org

[8] Behaghel, D., Secci, S., Vinapamula, S., Seo, S., Cloetens, W., Meyer, U., Contreras, L., Peirens, B., March 2017. Extensions for network-assisted mptcp deployment models. Internet-draft.
URL https://tools.ietf.org/id/draft-boucadair-mptcp-plain-mode-10.txt

[9] Benchaïb, Y., Secci, S., Phung, C., 2015. Transparent cloud access performance augmentation via an MPTCP-LISP connection proxy. In: Proceedings of the Eleventh ACM/IEEE Symposium on Architectures for networking and communications systems, ANCS 2015, Oakland, CA, USA, May 7-8, 2015. pp. 201–202.
URL https://doi.org/10.1109/ANCS.2015.7110140

[10] Boucadair, M., Jacquenet, C., Bonaventure, O., Henderickx, W., Skog, R., December 2016. Network-assisted mptcp: Use cases, deployment scenarios and operational considerations. Internet-draft.
URL https://tools.ietf.org/id/draft-nam-mptcp-deployment-considerations-01.txt

[11] Cable Map, 2017. Greg's cable map.
URL http://cablemap.info

[12] CAIDA, 2017. Archipelago (ark) measurement infrastructure.
URL http://www.caida.org/projects/ark

[13] Cisco, Sept 2016. Bgp best path selection algorithm. Cisco guide, Troubleshooting tech notes, Document ID:13753.
URL https://www.cisco.com/c/en/us/support/docs/ip/border-gateway-protocol-bgp/13753-25.html

[14] Coninck, Q. D., Bonaventure, O., 2017. Multipath QUIC: design and evaluation. In: Proceedings of the 13th International Conference on emerging Networking EXperiments and Technologies, CoNEXT 2017, Incheon, Republic of Korea, December 12 - 15, 2017. pp. 160–166.
URL http://doi.acm.org/10.1145/3143361.3143370

[15] Conti, M., Dragoni, N., Lesyk, V., 2016. A survey of man in the middle attacks. IEEE Communications Surveys and Tutorials 18 (3), 2027–2051.
URL https://doi.org/10.1109/COMST.2016.2548426

[16] Corbillon, X., Aparicio-Pardo, R., Kuhn, N., Texier, G., Simon, G., 2016. Cross-layer scheduler for video streaming over MPTCP. In: Proceedings of the 7th International Conference on Multimedia Systems, MMSys 2016, Klagenfurt, Austria, May 10-13, 2016. pp. 7:1–7:12.
URL http://doi.acm.org/10.1145/2910017.2910594

[17] Coudron, M., Nguyen, H. D. D., Secci, S., 2016. Enhancing buffer dimensioning for multipath TCP. In: 7th International Conference on the Network of the Future, NOF 2016, Búzios, Brazil, November 16-18, 2016. pp. 1–7.
URL https://doi.org/10.1109/NOF.2016.7810142

[18] Coudron, M., Secci, S., Maier, G., Pujolle, G., Pattavina, A., Nov 2013. Boosting cloud communications through a crosslayer multipath protocol architecture. In: 2013 IEEE SDN for Future Networks and Services (SDN4FNS). pp. 1–8.

[19] Coudron, M., Secci, S., Pujolle, G., Raad, P., Gallard, P., 2013. Cross-layer cooperation to boost multipath TCP performance in cloud networks. In: IEEE 2nd International Conference on Cloud Networking, CloudNet 2013, San Francisco, CA, USA, November 11-13, 2013. pp. 58–66.
URL https://doi.org/10.1109/CloudNet.2013.6710558

[20] Cyclops, 2017. Cyclops.
URL https://cyclops.cs.ucla.edu

[21] Di Battista, G., Erlebach, T., Hall, A., Patrignani, M., Pizzonia, M., Schank, T., 2007. Computing the types of the relationships between

autonomous systems. IEEE/ACM Trans. Netw. 15 (2), 267–280.
URL http://doi.acm.org/10.1145/1279660.1279662

[22] Elena, E., Rougier, J., Secci, S., 2010. Characterisation of as-level path deviations and multipath in internet routing. In: Next Generation Internet (NGI), 2010 6th EURO-NF Conference on, Paris, France, June 2-4, 2010. pp. 1–7.
URL https://doi.org/10.1109/NGI.2010.5534468

[23] Erlebach, T., Moonen, L. S., Spieksma, F. C. R., Vukadinovic, D., 2009. Connectivity measures for internet topologies on the level of autonomous systems. Operations Research 57 (4), 1006–1025.
URL https://doi.org/10.1287/opre.1080.0677

[24] Ford, A., Raiciu, C., Handley, M., Bonaventure, O., Jan 2013. Tcp extensions for multipath operation with multiple addresses. RFC 6824, RFC Editor.
URL https://tools.ietf.org/rfc/rfc6824.txt

[25] Frömmgen, A., Rizk, A., Erbshäußer, T., Weller, M., Koldehofe, B., Buchmann, A. J., Steinmetz, R., 2017. A programming model for application-defined multipath TCP scheduling. In: Proceedings of the 18th ACM/IFIP/USENIX Middleware Conference, Las Vegas, NV, USA, December 11 - 15, 2017. pp. 134–146.
URL http://doi.acm.org/10.1145/3135974.3135979

[26] Fuller, V., Farinacci, D., Jan 2013. Locator/id separation protocol (lisp) map-server interface. RFC 6833, RFC Editor.
URL https://tools.ietf.org/rfc/rfc6833.txt

[27] Furdek, M., Skorin-Kapov, N., 2012. Physical-layer attacks in transparent optical networks, optical communications systems. Http://www.intechopen.com/books/optical-communications-systems/physical-layer-attacks-in-transparent-optical-networks.

[28] Gao, L., 2001. On inferring autonomous system relationships in the internet. IEEE/ACM Trans. Netw. 9 (6), 733–745.
URL https://doi.org/10.1109/90.974527

[29] Goldberg, S., 2014. Why is it taking so long to secure internet routing? Commun. ACM 57 (10), 56–63.
URL http://doi.acm.org/10.1145/2659899

[30] Greenberg, A., 2014. Hacker redirects traffic from 19 internet providers to steal bitcoins.
URL https://www.wired.com/2014/08/isp-bitcoin-theft

[31] Hackdopi, 2017. Hackdopi.
URL http://hackdopi.wikidot.com

[32] IRR, 2017. Internet routing registries.
URL http://www.irr.net

[33] Jadin, M., Tihon, G., Pereira, O., Bonaventure, O., 2017. Securing multipath TCP: design & implementation. In: 2017 IEEE Conference on Computer Communications, INFOCOM 2017, Atlanta, GA, USA, May 1-4, 2017. pp. 1–9.
URL https://doi.org/10.1109/INFOCOM.2017.8057011

[34] Juniper, 2019. Configuring bgp to select multiple bgp paths. JUNOS 8.2 Routing Protocols Configuration Guide in Chapter 33 BGP Configuration Guidelines pp:571-572.
URL https://www.net.t-labs.tu-berlin.de/teaching/ss08/RL_labcourse/docs/04-juniper-bgp.pdf

[35] Kabbani, A., Vamanan, B., Hasan, J., Duchene, F., 2014. Flowbender: Flow-level adaptive routing for improved latency and throughput in datacenter networks. In: Proceedings of the 10th ACM International on Conference on emerging Networking Experiments and Technologies (CoNext). ACM.

[36] Kim, D.-Y., Choi, H.-K., 2016. Efficient design for secure multipath tcp against eavesdropper in initial handshake. In: Proceedings of the 2016 International Conference on Information and Communication Technology Convergence (ICTC 2016).
URL https://doi.org/10.1109/ICTC.2016.7763559

[37] Klöti, R., Kotronis, V., Ager, B., Dimitropoulos, X. A., 2015. Policy-compliant path diversity and bisection bandwidth. In: 2015 IEEE

Conference on Computer Communications, INFOCOM 2015, Kowloon, Hong Kong, April 26 - May 1, 2015. pp. 675–683.
URL https://doi.org/10.1109/INFOCOM.2015.7218436

[38] Kühne, M., 2012. Update on as path lengths over time.
URL https://labs.ripe.net/Members/mirjam/update-on-as-path-lengths-over-time

[39] Lange, A., March 2012. Issues in revising bgp-4. Internet-draft.
URL https://tools.ietf.org/id/draft-ietf-idr-bgp-issues-06.txt

[40] Li, M., Lukyanenko, A., Ou, Z., Ylä-Jääski, A., Tarkoma, S., Coudron, M., Secci, S., Fourthquarter 2016. Multipath transmission for the internet: A survey. IEEE Communications Surveys Tutorials 18 (4), 2887–2925.

[41] LIP6-MPTCP, 2017. open source project repository.
URL https://github.com/lip6-mptcp

[42] Misseri, X., Rougier, J., Saucez, D., 2012. Internet routing diversity for stub networks with a map-and-encap scheme. In: Proceedings of IEEE International Conference on Communications, ICC 2012, Ottawa, ON, Canada, June 10-15, 2012. pp. 2861–2866.
URL https://doi.org/10.1109/ICC.2012.6363982

[43] Nguyen, H. D. D., Phung, C., Secci, S., Felix, B., Nogueira, M., 2017. Can MPTCP secure internet communications from man-in-the-middle attacks? In: Conference on Network and Service Management, CNSM 2017, Tokyo, Japan, November 26-30, 2017. pp. 1–7.
URL https://doi.org/10.23919/CNSM.2017.8255970

[44] O.Bonaventure, C.Paasch, G.Detal, Jan 2017. Use cases and operational experience with multipath tcp. RFC 8041, RFC Editor.
URL https://tools.ietf.org/rfc/rfc8041.txt

[45] Oliveira, R. V., Pei, D., Willinger, W., Zhang, B., Zhang, L., 2010. The (in)completeness of the observed internet as-level structure. IEEE/ACM Trans. Netw. 18 (1), 109–122.
URL http://doi.acm.org/10.1145/1816288.1816297

[46] Peng, Q., Walid, A., Low, S. H., 2013. Multipath TCP algorithms: theory and design. In: ACM SIGMETRICS / International Conference on Measurement and Modeling of Computer Systems, SIGMETRICS '13, Pittsburgh, PA, USA, June 17-21, 2013. pp. 305–316.
URL http://doi.acm.org/10.1145/2465529.2466585

[47] Raiciu, C., Barré, S., Pluntke, C., Greenhalgh, A., Wischik, D., Handley, M., 2011. Improving datacenter performance and robustness with multipath TCP. In: Proceedings of the ACM SIGCOMM 2011 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications, Toronto, ON, Canada, August 15-19, 2011. pp. 266–277.
URL http://doi.acm.org/10.1145/2018436.2018467

[48] Raiciu, C., Paasch, C., Barre, S., Ford, A., Honda, M., Duchene, F., Bonaventure, O., Handley, M., 2012. How hard can it be? designing and implementing a deployable multipath tcp. In: Proceedings of the 9th USENIX Conference on Networked Systems Design and Implementation. NSDI'12. USENIX Association, Berkeley, CA, USA, pp. 29–29.
URL http://dl.acm.org/citation.cfm?id=2228298.2228338

[49] RIPE RIS, 2017. Ripe routing information service.
URL https://www.ripe.net/analyse/internet-measurements/routing-information-service-ris

[50] Routeviews, 2017. University of oregon route view projects.
URL http://www.routeviews.org

[51] Sankar, A. U. P., Poornachandran, P., Ashok, A., Krishnan, M. R., Hrudya, P., 2016. B-secure: A dynamic reputation system for identifying anomalous BGP paths. In: Proceedings of the 5th International Conference on Frontiers in Intelligent Computing: Theory and Applications - FICTA 2016, Volume 1. pp. 767–775.
URL https://doi.org/10.1007/978-981-10-3153-3_76

[52] Shaneman, K., Gray, S., 2004. Optical network security: Technical analysis of fiber tapping mechanisms and methods for detection and prevention. In: Proceedings of the IEEE MILCOM 2004. pp. 711 – 716.

[53] Starosielski, N., Yoo, D., Leong, R., Camacho, K., 2011. Critical nodes, cultural networks: Re-mapping guam's cable infrastructure. Amerasia Journal 37 (3), 18–27.
URL https://doi.org/10.17953/amer.37.3.m70071273lt62754

[54] Toonk, A., 2017. Bgpstream and the curious case of as12389.
URL https://bgpmon.net/bgpstream-and-the-curious-case-of-as12389/

[55] Tuexen, M., Stewart, R., Jan 2011. Stream control transmission protocol (sctp) chunk flags registration. RFC 6096, RFC Editor.
URL https://tools.ietf.org/html/rfc6096

[56] UNSD, 2017. Standard country or area codes for statistical use (m49).
URL http://unstats.un.org/unsd/methods/m49/m49regin.htm

[57] White, J., Pilbeam, A., 2011. An analysis of coupling attacks in high-speed fiber optic networks. In: Proceedings of the Enabling Photonics Technologies for Defense, Security, and Aerospace Applications VII.

[58] Witcher, K., 2005. Extensions for Network-Assisted MPTCP Deployment Models. White Paper, SANS Institute.
URL https://www.sans.org/reading-room/whitepapers/physical/fiber-optics-security-vulnerabilities-1648