Can MPTCP Secure Internet Communications from Man-in-the-Middle Attacks?

Ho-Dac-Duy Nguyen, Chi-Dung Phung, Stefano Secci, Benevid Felix*, Michele Nogueira*
Sorbonne Universités, UPMC Univ Paris 06, UMR 7606, LIP6, Paris, France. Email: firstname.lastname@upmc.fr
*Federal University of Paraná, Brazil. Email: {bfsilva,michele}@inf.ufpr.br

***Abstract*—Multipath communications at the Internet scale have been a myth for a long time, with no actual protocol being deployed so that multiple paths could be taken by a same connection on the way towards an Internet destination. Recently, the Multipath Transmission Control Protocol (MPTCP) extension has been 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 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.**

I. Introduction

The Multipath Transmission Control Protocol (MPTCP) [1] 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 layer, it is considered as the one having attracted the largest interest and deployment [2]. 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 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 load-balancers or multipath proxies [3] along the network can differentiate the route followed by the subflow packets.

Among the motivations pushed forward in support of MPTCP, there are (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 few years, the latter has almost never been explored 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 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 consider the case of MPTCP traffic source devices using two edge providers and we compare the obtained results on a geographical basis, identifying which countries and regions MPTCP may grant higher confidentiality with respect to MITM. An important assumption of our analysis is that the MPTCP scheduler behavior can be influenced so that it does not only look for throughput maximization, but also for path diversity exploitation for increased confidentiality, as investigated in [4].

The paper is organized as follows. Section II gives a background on MPTCP and related security concerns. In Section III, we describe our measurement methodology. Section IV presents the results, and Section V concludes the paper.

II. Background

A. MultiPath TCP (MPTCP)

MPTCP extends TCP and allows fragmenting a data flow from a single connection into multiple paths (subflows TCP) [1], [5], 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 [1]. The protocol improves the performance offered by a single flow and makes the connection more reliable using concurrent and redundant paths.

MPTCP employs a 4-tuple composed of source and destination IP address/port pairs to identify the different subflows [1]. MPTCP manages the creation, removal and utilization of the subflows while the connection is active. A MPTCP connection and its association with new subflows follow the same three-way-handshake as used for initiating a normal TCP connection. In the first handshake, MPTCP uses a control flag (MP_CAPABLE) in the option field of the segment header to verify if both end-hosts support MPTCP and configure the connection. If a remote host does not support the protocol, the connection seamlessly signals back.

978-3-901882-98-2

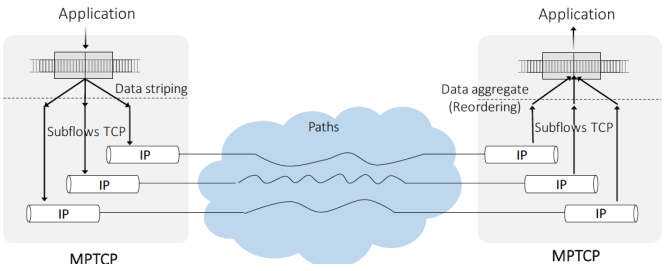


Fig. 1. Multipath TCP Connection: Overview

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 [6]. Finally, fragmenting data flow across different subflows makes flow hijacking difficult because attackers would need to capture the content transmitted through all the flows 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 on 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 primarily adopted not to improve communication performance or reliability, but to improve confidentiality. When addressing this feature, router-level path disjointedness can be considered as being too weak in particular against AS-level traffic capturing and route hijacking. We focus instead on AS-level path disjointedness.

B. 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 good enough to construct the transmitted data. In practice, it can be possible with optical layer attacks or by BGP route hijacking MITM attacks. At the optical layer, an attacker is able to split cables signal by using fiber optical taps, as described in [7]. Moreover, one can intercept the traffic by exploiting the coupling and out-of-the-fiber light propagation phenomena [8].

At the BGP layer, MITM attacks exploit the natural way BGP works. They stealthily hijack Internet traffic to modify or capture it before reaching the destination. BGP-based MITM attacks have been quite deeply studied for about twenty years; in a recent survey [9], the authors present a detailed description of such attacks, their effects as well as the methods of defense. 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 [10]: 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 the compromised host [11]. 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 [12]. The cost of such BGP incidents could be even more than what have been reported. Only notable ones are reported as in [13], [14]; 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 specification questions and challenges. There are attempts to verify the security of MPTCP [15], [16]. In [17], cryptography based solutions are proposed against eavesdropping. The authors in [16] present an analysis of residual threats in the MPTCP signaling and propose some fixes. Recently, an extension of MPTCP to secure the multipath communication was proposed in [18]; providing authentication and encryption mechanisms not only for the connection but also for the 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 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 [19]: 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, we attempt to provide a partial response to such questions.

III. 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 [20] for the sake of reproducibility.

A. Graph construction

We extract 2015 data from [21] (the latest dataset available), couple the AS-level topology with the inter-AS relationship data to form a new dataset containing all the AS links along

with their frequency of occurrence and relationship type. Comparing with other resources [22] [23], the topological data from [21] revealed to be more reliable and able to capture a broadened view of the Internet topology. Indeed, it integrates data not only from Routeviews [24], but also from other resources such as RIPE RIS [25]. Moreover, the traceroute-based approach employed in [22] has known issues [27] when converting router-level paths into AS-level. The inter-AS relationship data from [21] is extracted monthly from the Cyclops database [26], which combines BGP data with Internet eXchange Point (IXP) data and adopts the interference techniques proposed in [27].

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 which have a lower frequency being those used for backup operations or during BGP convergence periods. For the sake of consistency, we removed these unstable links.

B. Path diversity computation

The problem with selecting all the paths connecting two nodes over a graph that satisfies given routing properties is often referred to as policy-compliant path diversity computation in the literature [29] [30]. The common approach [29] is to convert the original graph into a type-of-relationship (ToR) graph [32], i.e., a directed graph in which the relationship between two adjacent vertexes is expressed via the direction of the edge connecting them, then 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.

We introduce a novel path search algorithm that leverage the scale-free characteristics [33] of the input AS graph (i.e., a graph with relatively few hubs capturing the majority of the paths) to optimize the execution time. In such 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 [34] (a bit lower in IPv6).

Searching for paths in a scale-free graph with a reasonable diameter is not too complex a problem when adopting breadth/depth-first search algorithms with a limited depth. From the constructed AS graph G, given two nodes s and d, the following breadth-first search strategy could be applied to discover all the policy-compliant paths between them in a reasonable time. Starting from the origin s, the algorithm explores each of the adjacent nodes n of s. A queue P is introduced to keep track of the explored paths; initially, it includes all the paths from s to n. Following these paths, the algorithm continues discovering the adjacent nodes to look for destination d. For a path p dequeued from P, the last node n is extracted, all of its neighbors are checked sequentially to determine the valid next hops towards d. A node is considered as valid once the path through it does not violate the valley-free routing property [28]. And a policy-compliant path is expressed using the following regular expression $c2p * p2p?p2c*$ [30] in which $c2p$, $p2p$ and $p2c$ express the relationship between interconnected nodes (where ? means that you can have zero or one p2p link).

In our constructed graph G, links are labelled according to the inter-relationship between nodes. 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 labelled as '$c2p$', '$p2c$' and '$p2p$', respectively. Then, 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).

Therefore by checking the labels of links along the explored path, the validity of next hops could 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.

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)
            NewPath ⟵ list(path)
            NewPath.append(n)
            if n = d then
                ValidPathSet.append(NewPath)
            if length(NewPath) = τ + 1 then break
            queue.append(NewPath)
        VisitedNode.add(v)
```

This path validation executes at run-time to ensure that non-compliant paths are detected at early stage, thus avoiding wasting time exploring invalid paths. And 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 limit the time and space complexity, but

also ignore selecting long paths which should be avoided in practice. Our algorithm is presented in detail in Alg. 1.

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 offline 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.

C. Source-destination pairs

Prior to evaluate the MITM robustness of MPTCP communications over the Internet, we first need to simulate such communication schemes on the AS graph. Thus, identifying source and destination of MPTCP communications.

The current Internet ecosystem is composed of more than 50 thousand ASes, out of which more than half are stub ASes, i.e., ASes that are origin or destination only 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) 'eyeball' ASes (hence excluding Internet carriers and stub ASes).

Rather than taking into account all possible communications, we target the connections among hosts at the edges, not performing short-lived communications but rather connections using multiple subflows. 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 and belongs to an AS at another country than the ones of the source.

Figure 2 illustrates an example of how we simulate MPTCP communications following the above procedure. For each two arbitrary edge provider ASes in a same country, one source is created (i.e., a dual-homed source). For an edge provider in an other country, one destination is used. Such a pair dual-homed source - single-homed destination defines the endpoints of a MPTCP communication. Listing all pairs, i.e., combining a given source with every destination, all possible (international) communications of a dual-homed host are covered. The robustness of that host connection against MITM attacks could be evaluated by the robustness of all communications originated from it. As previously mentioned, a communication is considered as more secure if there are more AS-disjoint paths between the two ends. The robustness of a communication is therefore relied on the level of path diversity; consequently the robustness of a source is evaluated by the average of the number of disjoint paths over all destinations. A formal definition of MITM robustness metric for a given source is provided in the next section.

Besides reducing the number of pairs to a reasonable and treatable number (requiring about one week of computation), it is worth noting that, in 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 multi-homed devices *uploading* to single-homed server as well as the case when single-homed devices *downloading* contents from servers connected to a multi-homed network.

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 servers connected to a multi-homed network; (iii) multi-homed devices communicating with another multi-homed device. A dual analysis, quite expensive computationally, covering these cases may be performed as well in future works.

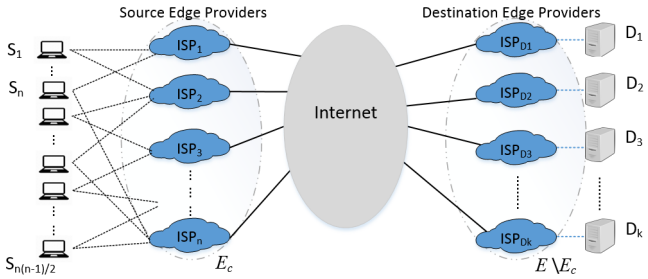


Fig. 2. Source-destination pair selection process

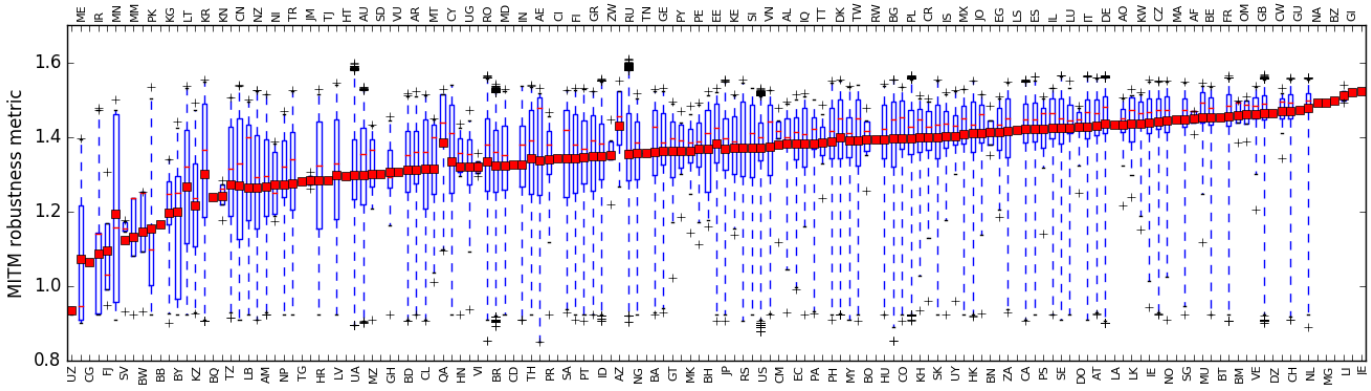
Let us more precisely characterize the source-destination pair election process. We segment the set of edge providers, E, in country-specific subsets, E_c, where c denotes a country in the set of countries C. We employ the AS-to-country mapping given by the CIDR Report [35]. Overall, for a given country $\tilde{c}$, the number of source-destination pairs is therefore equal to:

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

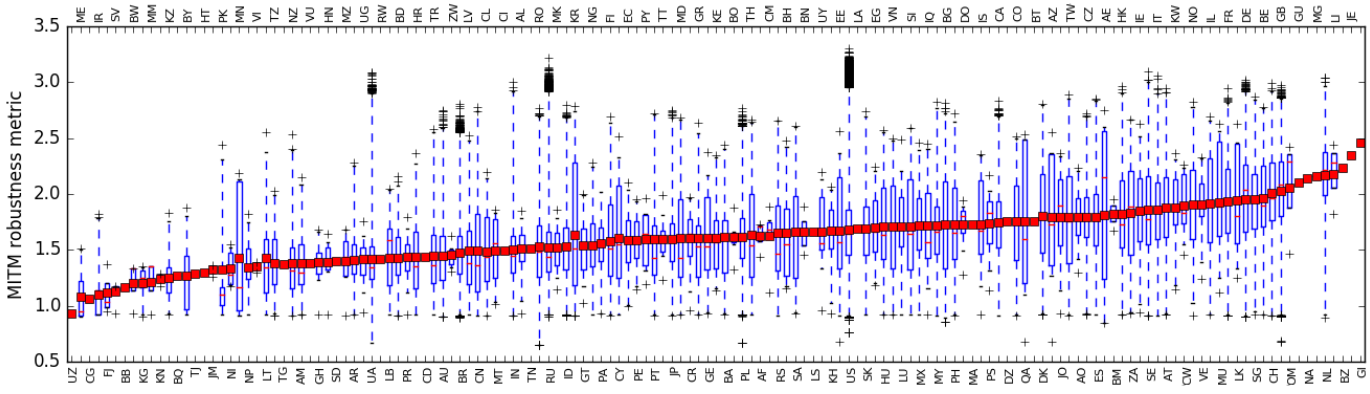
Doing so, we target a lower bound, pessimistic analysis, since we only take into consideration international communications and we suppose the destination is not multi-homed. The filter we set on the destination enumeration allows us to target communications that may need a higher level of confidentiality due to their international connotation. Moreover, in this way we also avoid a huge bias 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 [31]). 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.

IV. Results

We report the results obtained for a set of 147 countries, i.e., those countries from the United Nations statistics [36] that have at least two distinct edge providers officially based in the country (this excludes Greenland territories, very small city-state countries, many African countries and Indonesia). Our measurement approach can be summarized as follows:



(a) device view



(b) edge provider view

Fig. 3. MITM robustness distribution for 147 countries.

- For each country, we generate all possible dual-homed sources, i.e., all possible pairs of edge providers.
- For each source configuration (i.e., each pair of edge providers), we compute the number of disjoint paths to each destination. From each of the edge providers that are in a country different to the source, one destination is generated.
- *MITM robustness* metric: for a given source, we define it as the average of the number of disjoint paths over all the destinations: such metric can be considered as a level of unlikelihood that a MITM attack can take 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. For each country, a series of MITM robustness metrics, one for each source, is therefore created.

We characterize the resulting series using boxplot (with 0.1% outliers) distribution. We overlay over the boxplots the average of the corresponding series (red square), order them from left to right with increasing averages (average values do include outliers). We report the results in Figure 3, expressing two different viewpoints. Firstly, in Figure 3a, 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 path from this artificial source node toward destination. It provides 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. Secondly, in Figure 3b we provide an *edge provider view*, i.e., the MITM robustness is computed instead totaling up 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 additional AS-paths from the edge providers (by forms of load-balancing) can be made available to MPTCP subflows.

The above viewpoints also reflect different levels of trust on the providers. That is, while Figure 3b 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), Figure 3a assumes that attacks can happen at the source edge providers, hence revealing a low level of trust in source direct providers.

As a general assessment, Figure 3 shows that, considering 1.5 average as the rough threshold making the likelihood of MITM negative if higher than it, and positive if lower than it. 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 this likelihood positive for a majority of the countries. From an edge provider viewpoint, this ratio grows to roughly 60%, and higher than 90% if the edge provider choice is 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. Some minimum and even average values are below 1 because of the partial view over the Internet topology and the incompleteness of inter-AS relationship interference, which make some destinations unreachable (counted as 0 path); we left it in order 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.

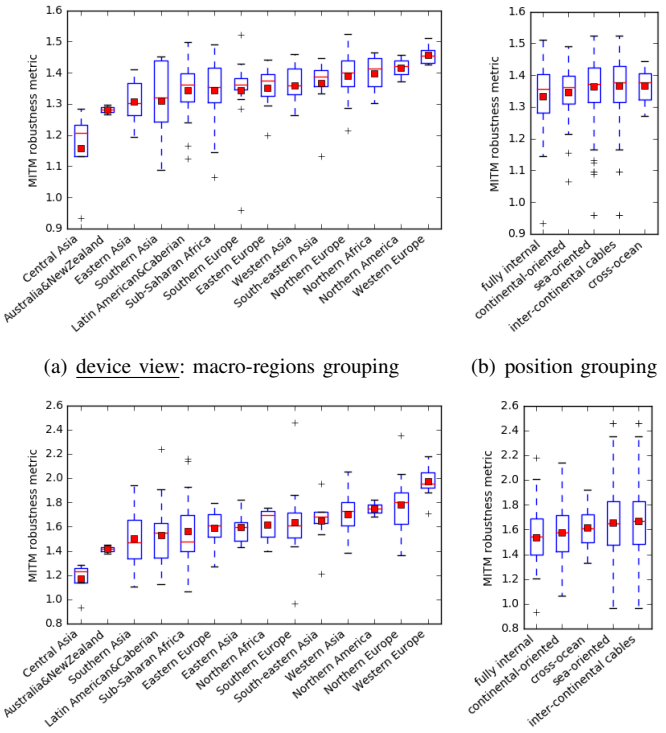
In addition, observing the plots in Figure 3, we can also remark that:

- 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 MPTCP 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 [37].
- 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 MPTCP to statistically expect high confidentiality for his communications regardless. 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.

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 4 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).

Western Europe appears to be the best off, followed by Northern Europe and Northern America. In almost 50% of Western Europe countries the edge providers maintains 2 disjoint paths to international destinations. The worst robustness is observed at Central Asia, then Australia & New Zealand; the reasons are likely network centralization practices and geographical isolation. A high variance is recorded at Southern Asia, Northern Europe and Sub-Saharan Africa indicating 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.



(a) device view: macro-regions grouping (b) position grouping

(c) edge provider view: macro-regions grouping (d) position grouping

Fig. 4. MITM robustness metric with aggregated country groups.

V. Conclusion

We explored in this paper how Internet path diversity could be exploited by means of multi-path transport protocols 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 MPTCP 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, MPTCP does not help in guaranteeing robustness against MITM attacks hence high confidentiality, unless the choice of the edge provider is carefully taken, or 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 and countries that are more obviously less robust against such attacks due to network centralization practices.

REFERENCES

[1] A. Ford et al., "TCP Extensions for Multipath Operation with Multiple Addresses," RFC 6824, Jan. 2013.

[2] O. Bonaventure, C. Paasch, G. Detal, "Use Cases and Operational Experience with Multipath TCP," RFC 8041, Jan. 2017.

[3] M. Boucadair et al, "Extensions for Network-Assisted MPTCP Deployment Models", draft-boucadair-mptcp-plain-mode-10, March 2017.

[4] M. Coudron, D. Nguyen, S. Secci, "Enhancing buffer dimensioning for Multipath TCP", *Proc. of NoF 2016*.

[5] Q. Peng, A. Walid, S. H. Low, "Multipath TCP algorithms: Theory and design," *Perform. Eval. Rev.*, vol. 41, no. 1, pp. 305–316, Jun. 2013.

[6] C. Raiciu et al., "Improving datacenter performance and robustness with multipath tcp," *Comp. Commun. Rev.*, vol. 41, no. 4, Aug. 2011.

[7] K. Witcher, "Fiber Optics and Its Security Vulnerabilities", White Paper, SANS Institute, 2005. 1st, 2017).

[8] J.S. White, A.W. Pilbeam, "An analysis of coupling attacks in high-speed fiber optic networks". In *SPIE Defense, Security, and Sensing*. International Society for Optics and Photonics, 2011.

[9] M. Conti, N. Dragoni, V. Lesyk, "A survey of man in the middle attacks," *IEEE Comm.Surveys & Tutorials*, vol. 18, no. 3, pp. 2027–2051.

[10] A. Pilosov, T. Kapela, "Stealing The Internet - An Internet-Scale Man In The Middle Attack," 2008 (online): https://www.defcon.org/images/defcon-16/dc16-presentations/defcon-16-pilosov-kapela.pdf (access: Apr. 1st, 2017).

[11] A. Greenberg, "Hacker Redirects Traffic From 19 Internet Providers to Steal Bitcoins," 2014 (online) https://www.wired.com/2014/08/isp-bitcoin-theft (access: Apr. 1st, 2017).

[12] A. Toonk, "BGPstream and The Curious Case of AS12389," 2017 (online) https://bgpmon.net/bgpstream-and-the-curious-case-of-as12389/ (access: Oct. 2nd, 2017).

[13] S. Goldberg, "Why is it taking so long to secure internet routing?" *Queue*, vol. 12, no. 8, pp. 20:20–20:33, Aug. 2014.

[14] A. U. Prem Sankar et al., "B-Secure: A Dynamic Reputation System for Identifying Anomalous BGP Paths", in *Proc. of FICTA 2017*.

[15] M. Bagnulo, "Threat Analysis for TCP Extensions for Multipath Operation with Multiple Addresses," RFC 6181, 2011.

[16] M. Bagnulo et al., "Analysis of Residual Threats and Possible Fixes for Multipath TCP (MPTCP)," RFC 7430, Jul. 2015.

[17] D. Y. Kim and H. K. Choi, "Efficient design for secure multipath TCP against eavesdropper in initial handshake," in *Proc. of ICTC 2016*.

[18] M. Jadin et al., "Securing MultiPath TCP: Design & Implementation," in *Proc. of IEEE INFOCOM 2017*.

[19] Hackdopi (website): http://hackdopi.wikidot.com (access: Apr.1st, 2017)

[20] LIP6-MPTCP open source project repository (website): https://github.com/lip6-mptcp (access: Apr. 1st, 2017).

[21] "AS-level Topology Archive" (website): http://irl.cs.ucla.edu/topology.

[22] CAIDA, "Archipelago (Ark) measurement infrastructure" (online): http://www.caida.org/projects/ark (access: Apr. 1st, 2017).

[23] Internet Routing Registries (website): http://www.irr.net (access: Apr. 1st, 2017).

[24] Routeviews, "University of Oregon Route View Projects," 2017 (website): http://www.routeviews.org (access: Apr.1st, 2017).

[25] RIPE RIS (website): https://www.ripe.net/analyse/internet-measurements/routing-information-service-ris (access: Apr.1st, 2017).

[26] Cyclops (website): https://cyclops.cs.ucla.edu (access: Apr. 1st, 2017).

[27] R.V. Oliveira et al., "The (in)path search of the observed internet AS-level structure," *IEEE/ACM Trans. on Networking*, vol. 18, no. 1, pp. 109–122, 2010.

[28] L. Gao, "On inferring autonomous system relationships in the internet," *IEEE/ACM Trans. on Networking*, vol. 9, no. 6, pp. 733–745, 2001.

[29] T. Erlebach et al., "Connectivity measures for internet topologies on the level of autonomous systems," *Operations Research*, vol. 57, no. 4, pp. 1006–1025, 2009.

[30] R. Klöti et al., "Policy-compliant path diversity and bisection bandwidth," in *Proc. of IEEE INFOCOM 2015*.

[31] B. Ager et al., "Anatomy of a large European IXP", in *Proc. of ACM SIGCOMM 2012*.

[32] G. Di Battista et al., "Computing the types of the relationships between autonomous systems," *IEEE/ACM Trans. on Networking*, vol. 15, no. 2, pp. 267–280, 2007.

[33] R. Albert and A. Barabsi, "Statistical mechanics of complex networks," in *Reviews of Modern Physics*, vol. 74, no. 1, pp.47, 2002.

[34] M. Khne, "Update on AS Path Lengths Over Time" (website): https://labs.ripe.net/Members/mirjam/update-on-as-path-lengths-over-time (access: Apr. 1st, 2017).

[35] T. Bates, P. Smith, G. Huston, "CIDR Report" (website): http://www.cidr-report.org (access: Apr. 1st, 2017).

[36] "Standard country or area codes for statistical use (M49)", (website): http://unstats.un.org/unsd/methods/m49/m49regin.htm (access: Apr. 1st, 2017).

[37] Cable Map (website): http://cablemap.info (access: Apr. 1st, 2017).

ACKNOWLEDGEMENT

This work was partially funded by the French Investissement d'Avenir FED4PMR project.