

# MIDAS: An Impact Scale for DDoS attacks

Rangarajan Vasudevan  
University of Michigan  
ranga@umich.edu

Z. Morley Mao  
University of Michigan  
zmao@umich.edu

Oliver Spatscheck  
AT&T Labs–Research  
spatsch@research.att.com

Jacobus Van der Merwe  
AT&T Labs–Research  
kobus@research.att.com

## I. INTRODUCTION

Distributed denial of service (DDoS) attacks are becoming increasingly common [1]. Even though DDoS attacks target end hosts, networks have to deal with increased traffic demands during attacks. In this work, we address the economic impact of DDoS attacks and provide a network centric *Measure of Impact of DDoS AttackS (MIDAS)* scale similar to systems used to classify the impact of earthquakes and tornadoes. Our motivation is that such a classification scheme can be used by *any network operator* to assess the severity of a DDoS attack, and allow comparisons. Currently, a common way of characterizing DDoS attacks is in terms of measures such as packets per second (pps) or bits per second (bps). Such simple measures are misleading as, for instance, a 100Mbps attack against a well-provisioned server in a data center is negligible in impact compared to the same attack against an end-host connected through a cable modem. Making the classification concrete in terms of the actual economic impact increases incentives to proactively mitigate DDoS attacks from an operator’s perspective. Furthermore, a classification scheme will lead to improved understanding of the properties of DDoS attacks that have direct impact on the networks. Ultimately, such a scheme provides valuable insights into evaluating and designing mitigation schemes.

Two real world examples that inspire our approach, namely the Richter scale for earthquakes and the Fujita scale for tornadoes, serve to illustrate two different approaches: measuring attributes of the event directly, versus, measuring the impact of the event. The Richter scale measures the magnitude of an earthquake by estimating the energy released from the motion of tectonic plates. That is, it measures the *size* of an earthquake, regardless of whether it caused any damage or not. The Fujita scale, on the other hand, estimates the actual damage caused by a tornado based on surveys conducted afterward. It therefore estimates the *impact* of a tornado rather than the size. So for example, a large tornado that causes minimal damage to man-made structures will not have a significant magnitude on the Fujita scale.

We argue that an approach similar to the Fujita scale is appropriate for a DDoS attack impact scale. Intuitively, a large DDoS attack that impacts a single end-user is of less interest than a very small attack (*e.g.*, a single packet exploit) that causes a router to crash thus impacting many end-users. Our specific interest is to develop a DDoS attack impact scale, the MIDAS scale, from a network service provider’s perspective. We would like to gauge the actual impact of DDoS attacks to rank the relative importance of attacks which

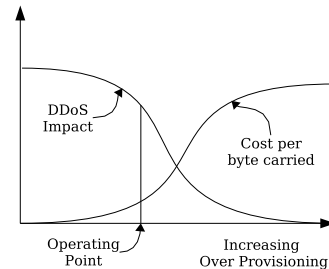


Fig. 1. Cost per-byte-carried and DDoS Impact as a function of network over-provisioning

could then be used, for instance, to determine priority for mitigation strategies. Our approach is to estimate the actual or potential *economic* impact of DDoS attacks to drive our MIDAS metric estimation. Rather than absolute values, we believe that a *relative* metric provides an intuitive indication of the severity of impact regardless of provider size. Thus, the same MIDAS metric should represent the same relative economic impact across different providers. Our scale is applicable to ISPs of all sizes and diverse tiers.

We present models to calculate the MIDAS scale using comprehensive economic and network data. However, obtaining the necessary data to calculate them precisely is in general infeasible. Therefore, we also indicate how the MIDAS scale can be estimated in practice.

## II. WHY AN IMPACT METRIC?

While typically aimed at specific end-systems, DDoS attacks can also impact the networks that carry the attack traffic and therefore, can indirectly impact other network users. This collateral damage implies that a holistic network-wide view of DDoS attacks is necessary to fully assess their impact. Ideally, such an assessment should span all impacted networks (*e.g.*, crossing AS boundaries). While appropriate information sharing would help realize such an eventuality, our immediate focus is at the more pragmatic single provider case. In this Section we motivate our decision to develop a DDoS scale based on the *impact* of an attack. Specifically we attempt to illustrate that while there is a cost involved in carrying all DDoS traffic, only some DDoS attacks impact the network and its users.

IP networks are typically provisioned based on some pre-determined engineering rules involving the observed aggregate and peak link utilization [2]. Note that the observed traffic load includes both regular and DDoS traffic. IP networks have to be *over-provisioned* because of the unpredictability

and changing nature of the offered traffic load. The *per-byte-carried cost* of a particular network increases as the amount of over-provisioning in a network increases. This is illustrated graphically in Figure 1. For brute force DDoS flooding attacks it is possible (at least in theory) to increase the over-provisioning in a network to the point where DDoS attacks have no impact on the network or its users, except for the actual target of the attack. Intuitively, (and shown in Figure 1), as the amount of over-provisioning in a network decreases, the impact of DDoS attacks increases.

At any moment in time a network operates at some point along the X-axis. The exact operating point is determined by both the available capacity (amount of over-provisioning) and the offered load. For example, if the offered load stays the same, an increase in capacity would move the operating point to the right, thus increasing the per-byte-carried cost and decreasing the impact of DDoS attacks. This discussion illustrates the trade-off network operators face between reducing the operational costs of running a network and increasing the robustness of the network against DDoS attacks. Furthermore, while we framed the argument in the context of increased capacity, it would apply equally well to cost involved in using other DDoS mitigation mechanisms (*e.g.*, dedicated DDoS filtering devices).

Interestingly, in a best-effort network like the Internet the network operator typically does not directly pay any of the costs involved in carrying DDoS traffic. As outlined above, the costs for the operator are operational in nature (due to increasing the capacity of the network). For flat-rate billing models, this increased cost would effectively reduce the operator's income. However, for usage-based billing models, the operator's income typically increases with increase in traffic, be it good or bad. This implies that the main driver for a large provider to address the DDoS issue is *not* the billing model but the potential loss of revenue when customers become dissatisfied with the provided service due to DDoS attacks.

This situation is slightly different for small network operators which typically pay a usage based fee for their uplinks to higher tier network operators (for example tier-2 ISPs paying tier-1 ISPs). This usage based uplink fee increases as the DDoS traffic on the uplinks increase. However, even the small network operators typically receive more usage based fees from their customers than they pay the higher tier network operators for uplink services. Therefore, as long as the DDoS traffic either originates or targets customers of the network operator the increased cost of DDoS traffic carried over the uplink is covered directly by increased revenues from customers. For these reasons we ignore this component in the MIDAS scale.

### III. IMPACT OF DDoS ATTACKS

As outlined in the previous section, the MIDAS scale of DDoS attacks focuses on capturing the cost of a DDoS attack in the context of a particular network. Similar to the Fujita scale, we exclude long-term costs, such as network upgrades or deployment of DDoS mitigation equipment, from the attack costs. In our approach we focus on the potential

economic impact of DDoS attacks on the network provider given a specific network. Specifically, we consider the *cost of SLA violations* and the *cost of losing customers* as the potential economic impacts to be captured in the MIDAS scale.

In this section, we discuss both an accurate but impractical model of computing these costs and our MIDAS scale, as well as a simpler practical model which approximates these values. The practical model computes what we call the MIDAS2007 scale. We anticipate that the assumptions we make in translating the MIDAS scale into the MIDAS2007 scale might not hold indefinitely. Therefore, we expect that similar to the SPEC CPU benchmarks new MIDASXXXX scales will appear over time, even though the underlying principles presented in the MIDAS scale itself are preserved. Finally, in section IV, we derive estimates for the MIDAS scale which depends only on direct network measurements. Because it can be calculated from network measurements, this MIDAS2007NET scale offers a pragmatic way of calculating the impact of DDoS attacks while still being based on the underlying economic impact of such attacks.

#### A. SLA violation cost

Network operators can provide arbitrary SLAs to their customers and these could be violated in arbitrary ways by a DDoS attack. So, judging the cost impact of DDoS attacks based on SLA violations is a very network specific task. An exact calculation of this SLA cost,  $C_{SLA}$ , of a given DDoS attack requires knowledge of all SLAs a network provider offers to all customers and calculating the sum of all penalties of the violated SLAs. We define  $Penalty(SLA_i, c)$  to be the penalty of violating  $SLA_i$  for a particular customer  $c$ . Therefore  $C_{SLA}$  can be computed as follows:

$$C_{SLA} = \sum_{c,i} Penalty(SLA_i, c) \quad \forall i, \text{ if } SLA_i \text{ is violated.}$$

One could argue that such a network specific cost should not be captured in a DDoS attack impact scale. However, we reason in its support since this cost is indicative of how well a network operator can deliver on its promised SLAs under adverse conditions. Intuitively network operators who provide SLAs carelessly will experience higher rated DDoS attacks, indicating to potential customers that they have a higher DDoS related risk.

As pointed out, in general, SLA violation costs can be rather arbitrary. So, in the context of MIDAS it would be useful if we could approximate typical SLA violation costs without having to assess all SLAs a network operator might have provided. We investigated, using resources on the Web, the SLAs that are typically offered by today's tier-1 network operators. We found most SLAs to be framed based on one or more of the following properties: (i) Network-wide performance: in terms of network availability or network downtime, latency, loss rate, and jitter in the form of traffic matrix across major cities with a threshold value for each based on monthly averages. (ii) Reliability: site to site reliability, backbone reliability. (iii) Packet delivery guarantee: between the hub routers within the backbone network, the packet delivery rate is above a certain threshold. (iv) Outage reporting guarantee: customer is notified within a certain

amount of time of his equipment becoming unavailable. (v) Power availability: power to customer’s servers should be adequate for at least a certain duration of time.

Analyzing the nature of these metrics we notice that most of them are network-wide properties. The exception is the power availability. Fortunately violations of this SLA are most likely not related to DDoS attacks. Also, SLAs help translate measurements of these network-level properties into economic costs.

From analysis of industrial practices, we find that penalties paid to a customer for an SLA violation often range from one day to one month of the revenues generated by the customer. Therefore, we can approximate  $C_{SLA_i}$  by computing  $C^{2007}_{SLA_i}$ , the cost of violating  $SLA_i$  as follows (where  $Rev(c, T)$  is the current revenue within a recent time period  $T$  of customer  $c$  having an  $SLA_i$ ):

$$C^{2007}_{SLA_i} = \sum_c Rev(c, T)$$

In accordance with our observations, the time period  $T$  is chosen between one day and one month.

Using this formula, we can approximate DDoS-related SLA violation costs simply by determining if a DDoS attack violated a network-wide SLA and computing the sum of revenues of customers associated with this SLA for time period  $T$ . For the MIDAS2007 scale we choose  $T$  to be one day which is the most common case for violations of network-wide SLAs. Then, assuming that a network provider has multiple  $SLA_i$ , we compute  $C^{2007}_{SLA}$  as the sum of all  $C^{2007}_{SLA_i}$  for which  $SLA_i$  was violated because of a DDoS attack.

### B. Risk cost

The risk cost captures the risk of a DDoS attack causing such disruption to a customer that he leaves the network. This directly affects the future revenues of the network operator. These costs can be estimated by the following formula (where  $Risk(c)$  is the probability that customer  $c$  would leave a network due to DDoS attacks,  $Rev_{future}(c)$  is the future revenue for the provider from a customer  $c$ ,  $C_{risk}(c)$  is the cost to a provider of customer  $c$  leaving, while  $C_{risk}$  is the cost across all customers):

$$C_{risk}(c) = Rev_{future}(c) * Risk(c)$$

$$C_{risk} = \sum_c C_{risk}(c) \forall c \text{ if } c \text{ is impacted.}$$

Unfortunately it is impractical to exactly measure either value. We attempt to approximate their values as follows:

1) *Customer Revenue at Risk*: The  $Rev_{future}(c)$  depends on customer  $c$ ’s future choice of network operators as well as future traffic volumes generated by the customer. This partly depends on external factors. For example, the customer might decide to switch network operators within the next month because of a cheaper service from another network operator. Hence, losing this customer now because of a DDoS attack has a small impact. On the other hand, a customer might have stayed with the network operator for years to come and,

therefore, losing this customer has a high impact on future revenues.

To approximate this cost, we assume that the current revenues from a customer holds for a fixed time interval in the future and then calculate  $Rev_{future}(c)$ . Since most contracts have a one year minimum term, we fix the time interval as one year into the future. We now have a formula for estimating revenue from a customer as:

$$Rev_{2007_{future}}(c) = Rev(c, 1month) * 12$$

2) *Risk of Customer Leaving*: The risk of a customer leaving is in general hard to calculate. A customer might leave because his traffic is impacted by a DDoS attack targeted at another customer (collateral damage) or, because he is the target of an attack and another network operator provides superior DDoS mitigation techniques. In either case, the customer leaves in the quest for better service in the face of DDoS attacks. On the other hand, a customer might also leave because the economical impact of a DDoS attack is so large that it is no longer economically viable for him to continue with the same network provider. For example, an e-tailer who is continuously DDoSed during Christmas season might not have enough cash to survive.

In short, the risk of a customer leaving is a function of, (i) attack scope: how much customer traffic is impacted, (ii) attack duration: for how long customer traffic is impacted, and (iii) attack frequency: how frequently a customer is impacted by DDoS attacks.

If any of these values increases, the likelihood of the customer leaving also increases. Unfortunately it is hard to accurately model customer behavior. For instance, if customers were to be asked what level of DDoS they would be willing to tolerate, they are likely to suggest numbers that are much lower than what would be the case in practice. On the other hand, there is not enough empirical data available to model what customers will actually do. This leaves us with modeling customer behavior based on domain knowledge and what we believe are reasonable assumptions. Specifically, we make the following assumptions to estimate the risk of a customer leaving:

- We consider a customer to be impacted if at least 1% of its traffic is impacted. By “impacted”, we mean that application specific performance requirements such as maximum loss rate and jitter are not satisfied. This choice of 1% is motivated by the fact that most customers would not notice if less than 1% of their traffic is impacted (considering that on the Internet some traffic is always adversely impacted due to, for example, routing changes or congestion).
- Intuitively we expect a customer’s dissatisfaction with DDoS related impact to grow as a non-linear function of the duration of the attack. To model this, we bin the duration of the attack in 10 minute bins. This is reasonable since routing events on today’s Internet typically are on the order of a few minutes. So DDoS attacks of shorter durations are typically not distinguishable from routing events from the customer’s perspective, and all Internet users tolerate these events today. An exponential

increase in risk based on attack durations captures the fact that the longer an attack impact persists the more likely the customer will be dissatisfied enough to leave.

- We model the impact of attack frequency also as an exponential increase. We consider the last 12 months to count the number of attacks which impacted a particular customer. We consider 12 months to be a reasonable compromise between taking recent events into account and aging out events that happened in the more distant past. For example, an e-tailer who experienced an impact over the previous Christmas season is likely to remember it in the current season, but without any further incidents it might be less concerned the next season. We again choose an exponential increase because we expect customers to become increasingly annoyed if outages are repeated frequently.

Since both frequency of attacks as well as duration of an attack instance dictate a customer's experience with a provider, we add these factors together in the exponent term. Using these assumptions we can estimate the risk of a customer leaving as follows (where BaseRisk is the risk of a customer leaving given a base attack scenario).

```
// for a DDoS attack a, with duration d:
// AttackCnt(c, T) = Number of attacks impacting
// >= 1% of c's traffic in recent T time period.
If (a impacts < 1% of customer c's traffic)
  Risk2007(c) = 0
else {
  BinCnt = ⌊d/10min⌋
  HistoryCnt = AttackCnt(c, 12months)
  Risk2007(c) =
    1 - ((1 - BaseRisk)(BinCnt+HistoryCnt))
}
```

For the MIDAS2007 scale, we define the base attack scenario as the case where more than 1% of a customer's traffic is impacted for less than 10 minutes occurring only once within the last 12 months. We estimate this value by conservatively assuming that a customer would leave with 99.999% probability if in the last 12 months his service is interrupted every day for at least one hour. This translates into a BaseRisk of 0.031.

### C. The MIDAS scale

Using the cost models derived in the previous sections we can now calculate the cost of a DDoS attack within a particular network as the sum of SLA violation cost and risk cost:  $C_{DDoS} = C_{SLA} + C_{risk} + C_{uplink}$ , which can be approximated in practice using the assumption made earlier as:

$$C^{2007}_{DDoS} = C^{2007}_{SLA} + \sum_c [Risk^{2007}(c) * Rev^{2007}_{future}(c)]$$

which can be computed by a network operator. To calculate the MIDAS scale value that is globally applicable, we normalize the cost of an attack by the overall revenues of a network provider. The revenues of the network operator have to be calculated over a certain amount of time. In

the context of the desired properties of the MIDAS scale, this duration can be arbitrarily chosen since it only linearly increases/decreases the MIDAS scale value. To avoid short time revenue events and to match our risk cost estimation, we choose the revenue of the network operator in the prior 12 months as the normalization factor. Thus the MIDAS scale factor (SF) is defined as:

$$MIDAS_{SF} = \frac{C_{DDoS}}{NetworkTotalRevenue(12months)}$$

Since the true MIDAS SF is expected to be hard to compute, we expect network operators to calculate and compare the approximate MIDAS values instead. Our approximation is defined as:

$$MIDAS^{2007}_{SF} = \frac{C^{2007}_{DDoS}}{NetworkTotalRevenue(12months)}$$

In the next section we introduce a MIDAS value calculation where the estimation is based purely on network observations.

## IV. MIDAS2007NET

Even though the MIDAS2007 impact factor discussed in the previous section can be realistically computed on most networks, it typically requires several data sources maintained by multiple organizations. For example, traffic impact needs to be measured on the network, whereas past revenues have to be collected from the accounting organization. In many large organizations, establishing this level of accurate and reliable collaboration is cumbersome. Therefore, we propose a variant of the MIDAS2007 factor called the MIDAS2007NET which can be computed based on network data alone. Even though this factor is not directly comparable with the MIDAS2007 factor, it preserves the same desirable properties.

The basic intuition behind the MIDAS2007NET factor is that provisioned bandwidth is roughly proportional to actual traffic volumes seen on the network which are roughly proportional to the revenues associated with them. So we do the following:

- The total revenues of a network provider is replaced by the sum of the link capacities at the perimeter of the network, *totalcapacity*, i.e., the link capacities of all customer/peer facing access router interfaces. Instead of using traffic volume information, link capacities are used as they are closely associated with traffic volume and revenues.
- The total revenues from a customer *c* is replaced by the total link capacity of all access interfaces *c* connects to (*customercapacity(c)*). Since most networks have a provisioning database which associates customers with access interfaces, this number can be easily computed.
- We assume that all customers are subscribed to all network-wide SLAs of the provider.
- We assume a customer is impacted if more than 1% of the customer's peak traffic volume in the last 10 minutes would have to traverse any core or access link which is experiencing a loss rate of 5% or more. (It has been shown that a 5% loss rate becomes problematic for TCP

connections [3].) Links with larger than 5% loss rate can be determined easily by the network operator by SNMP-polling the appropriate router interface MIBs. Then a customer traffic matrix computed based on Netflow data or by network tomography tools can be used to detect the fraction of each customer's traffic impacted by any such link. Therefore, the only information which is difficult to gather and is required to determine customer impact is to decide if the high link loss rate was caused by a DDoS attack or another network event. We use a conservative estimate and assume all such link events, which cannot be explained by non-DDoS related causes, to be DDoS related.

These approximations result in the following formulas (as a modification of the MIDAS2007 formulas in the earlier section):

$$\begin{aligned}
 C2007\_net_{SLA_i} &= totalcapacity \\
 Rev2007\_net_{future}(c_i) &= customercapacity(c_i) \\
 C2007\_net_{DDoS} &= C2007\_net_{SLA} + \\
 \sum_i [Risk2007(c_i) * Rev2007\_net_{future}(c_i)] \\
 MIDAS2007NET &= \frac{C2007\_net_{DDoS}}{totalcapacity}
 \end{aligned}$$

Notice that the  $C2007\_net_{SLA_i}$  is equal to  $totalcapacity$  due to the fact that we assumed that all customers are subscribed to all network wide SLAs. So, if any such SLA is violated the network produces no revenues. Because it can be calculated directly from network measurements, we use the MIDAS2007NET scale for our evaluation presented in Section V.

## V. EVALUATION OF THE MIDAS SCALE

In this section we describe our experiences in using the MIDAS scale in realistic network topologies and show the sensitivity of the scale. Using simulations [4], we demonstrate the usefulness and validity of the MIDAS scale by showing that it qualitatively conforms to our expectation of attack impact.

To recap from Section IV, the MIDAS2007NET was calculated using  $customercapacity(c)$  as the  $Rev2007\_net_{future}(c_i)$  and  $totalcapacity$  as the term  $C2007\_net_{SLA_i}$ . We now describe how we calculate the values of these two terms. In our experiments, we evaluate the impact of an attack on a customer by considering impact on the customer traffic flows (as defined in our earlier work [4]). A traffic flow from a customer is said to be impacted or affected if at least one link it traverses is overloaded by the attack. If a customer flow is affected, then the capacity of the access link used by that particular flow to enter into the network is added to the  $customercapacity(c)$  term. The  $customercapacity(c)$  is now the sum of capacities of all access links (counted uniquely) that carry at least one affected customer flow. As before, the term  $totalcapacity$  is the sum of capacities of all access links of the network.

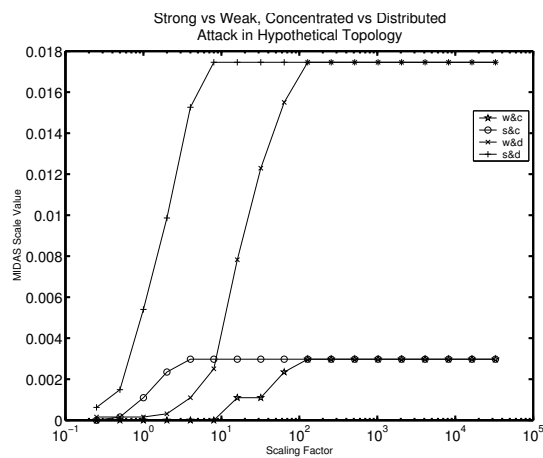


Fig. 2. Behavior of various attack instances in a hypothetical setting

Since we are more interested in the relative differences in MIDAS scale values, we do not consider the contribution of SLA violation costs to the  $MIDAS2007NET$  value. This is because this contribution is constant for all attacks and can thus be safely ignored for computing relative values. Thus,  $MIDAS2007NET$  is dependent upon the total number of affected flows in the network. The higher the number of impacted flows, the more likely it is that the term  $customercapacity$  is larger, increasing the  $MIDAS2007NET$  value.

We adopt the following categorization of attacks for our evaluation:

- A **strong and concentrated** attack denotes an attack that originates from a few sources, and targets a few destinations with a large volume (without any attack scaling) thus overloading a small number of network links (denoted by **s&c**).
- Likewise, a **weak and concentrated** attack has a much lower attack volume compared to its strong counterpart while sharing the same concentrated property (denoted as **w&c**).
- A **strong and distributed** attack originates from multiple sources, usually spread across the network, and targets several destinations that are typically spread across various regions in the network thus overloading a large fraction of network links (denoted as **s&d**).
- The combination of **weak and distributed** properties of an attack is denoted as **w&d**.

Thus, for example, an **s&d** attack overloads more links impacting more customers and is therefore expected to have a high MIDAS value.

### A. Results

We use a hypothetical topology modeled to reflect population density on the US sub-continent for our evaluation. Figure 3 shows a sample of the hypothetical topology where each vertex on the rectangle abstracts the PoP and the numbers on the vertices reflect the sizes of the PoPs. In this depiction, only the PoP labeled as 1 is expanded into its constituent hub and access routers. A similar hierarchical topology holds for other PoPs as well with the number of routers and the link capacities determined by the size of

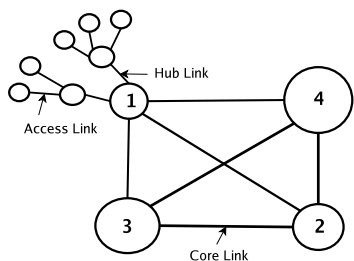


Fig. 3. A depiction of the hypothetical topology

the PoP. So, for example, the vertex numbered 1 pertains to the PoP in the hypothetical topology with the lowest traffic-carrying capacity reflecting a low population density.

In this setting, attacks were designed for specific purposes to better illustrate the behavior of MIDAS scale under expected conditions. A strong attack (when not scaled) was designed to occupy nearly 12 times as much bandwidth as a weak attack. On the other attack dimension, a distributed attack originated from at least 5 sources picked from at least 2 PoPs and attacked at least 5 targets in at least 2 PoPs. While, a concentrated attack originated from at most 2 sources both of which are within the same PoP, targeting at most 2 targets again co-located in the same PoP. These numbers were chosen mainly to provide a clear picture of the behavior of the MIDAS scale.

Figure 2 compares various categories of attacks in this hypothetical setting. Here the distinction between a strong and a weak attack is only that at a scaling factor of 1.0, a strong attack utilized a larger percentage of access link capacity as opposed to a weak attack. In other words, both attacks involve the same sets of sources and targets. Due to the above similarity, attacks belonging to the same concentrated or distributed category have the same maximum impact. However, the strength of the attack dictates how early the maximum impact plateau is reached. Thus, the **s&d** attack overloads a set of access links as well as a few core links and thus its impact curve rises sharply as opposed to the **w&d** attack that impacts usually a smaller number of links at a time resulting in a more gradual increase with more steps. A similar behavior is observed in the domain of concentrated attacks but, of course, these have a much smaller maximum impact plateau value.

Using the above experiments, we have mapped the intuitive behavior of the MIDAS scale. The above discussions also serve to indicate that small access links, though providing low capacities for legitimate customers, also serve a restricting role for bandwidth intensive attacks. The MIDAS scale captures this restriction in the plateaus of the curves.

## VI. RELATED WORK

The field of service pricing to address congestion and resource allocation issues in networks is popular among researchers. However, to the best of our knowledge, there has been no known previous technical work targeted at measuring the economic cost of the impact of DDoS attacks. The only other work that comes close to our focus in this paper is [5], where the authors provide a purely technical framework for modeling attacks and their impacts on networks (using a

probabilistic state transition matrix to model the response of the system to a network attack). Related to our effort, from the perspective of evaluating the quality of service in IP networks, Diot *et al.* [6] defined a new metric defining service availability in the presence of link failures. Recent research has focused on building better models to understand DDoS attacks like in the case of [7] where the authors consider the network flow model. Though not directly related to DDoS impact cost measurement, [8] provides an economic analysis of DDoS defense mechanisms. On the completely economic front, the Incident Cost Analysis and Modeling Projects (I-CAMP) I and II [9] dealt with calculating user costs due to disruptive incidents. [10] presents a purely financial framework for measuring the cost incurred due to an attack in terms of loss and recovery effort.

## VII. CONCLUSION

We have described an abstract framework to compute a network operator-centric impact scale for DDoS attacks, the MIDAS scale. We derived estimations of the cost functions to compute this scale value based on both economic and network data (MIDAS2007), as well as network data alone (MIDAS2007NET). We validated the MIDAS2007NET metric using real and hypothetical network topologies and DDoS data. Such practical estimations are designed to benefit service providers by allowing network operators to rank DDoS attacks in terms of impact using MIDAS and prioritizing the use of resources and personnel; and, compare mitigation strategies for DDoS attacks to understand their effectiveness based on MIDAS scale values. We believe that MIDAS is the first important step towards a DDoS attack impact scale of global relevance, and as researchers obtain additional insights, new incarnations of the MIDAS scale are expected to arise while adhering to the model outlined in this paper.

## REFERENCES

- [1] R. Richmond, "Firms Join Forces Against Hackers," *Wall Street Journal*, March 28, 2005.
- [2] J. Boyle, V. Gill, A. Hannan, D. Cooper, D. Awduche, B. Christian, and W. Lai, "Applicability Statement for Traffic Engineering with MPLS." RFC3346, August 2002.
- [3] J. Padhye, V. Firoiu, D. Towsley, and J. Kurose, "Modeling TCP Throughput: A Simple Model and its Empirical Validation," in *Proceedings of SIGCOMM'98*, 1998.
- [4] R. Vasudevan, Z. Morley Mao, O. Spatscheck and J. van der Merwe, "Reval: A tool for real-time evaluation of ddos mitigation strategies," in *USENIX Annual Technical Conference*, 2006.
- [5] S. D. Moitra and S. L. Konda, "A Simulation Model for Managing Survivability of Networked Information Systems," in *CMU Technical Report CMU/SEI-2000-TR-020*, 2000.
- [6] C. Diot, G. Iannaccone, A. Markopoulou, C.-N. Chuah, and S. Bhattacharyya, "Service availability in IP networks." Sprint ATL Research Report RR03-ATL-071888, Sprint ATL, July 2003.
- [7] J. Kong, M. Mirza, J. Shu, C. Yoedhana, M. Gerla, and S. Lu, "Random Flow Network Modeling and Simulations for DDoS Attack Mitigation," in *Proc. ICC*, 2003.
- [8] Y. Huang, X. Geng, and A. B. Whinston, "Defeating DDoS Attacks by Fixing the Incentive Chain," *ACM Trans. on Internet Technology*, 2006.
- [9] V. Rezmierski, A. Carroll, and J. Hine, "Incident Cost Analysis and Modeling Project (I-CAMP II) - A Report to the USENIX Association," in *ICAMPReport2*, 2000.
- [10] T. Dübendorfer, A. Wagner, and B. Plattner, "An Economic Damage Model for Large-Scale Internet Attacks," *Proc. IEEE Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises*, 2004.