Exploiting Internet Delay Space Properties for Sybil Attack Mitigation

Bo Zhang and T. S. Eugene Ng
Rice University

ABSTRACT

Recent studies have discovered that the Internet delay space has many interesting properties such as triangle inequality violations (TIV), clustering structures, and constrained growth. Understanding these properties has so far benefited the design of network models and network-performance-aware systems. In this paper, we consider an interesting, previously unexplored connection between Internet delay space properties and network locations. We show that this connection can be exploited to mitigate the Sybil attack problem in peer-to-peer systems.

1. INTRODUCTION

Recent studies [25, 14, 23, 15] have identified many interesting properties of the Internet delay space[1], such as triangle inequality violations (TIV), clustering structures, and constrained growth. With the increased understanding of Internet delay space properties, researchers have started applying them to solve some practical problems. For examples, [25] proposes a network delay model that takes the delay space properties into account, [23] improves the performance of two neighbor selection systems by making them TIV-aware, and [16] proposes a routing overlay that exploits TIV to select the best peerings.

In this paper, we consider an interesting, previously unexplored connection between Internet delay space properties and network locations. We show that this connection can be exploited to mitigate the Sybil attack problem in peer-to-peer (P2P) systems.

1.1 The Sybil Attack

The Sybil attack exploits the fact that in a P2P system, peers are distinguished by their logical identities. Thus a node with two logical identities is treated as two distinct peers by the system. In a Sybil attack, a malicious node manufactures a large number of distinct logical identities (called Sybil identities) and uses them to join a P2P system. Left unchecked, these Sybil identities can disrupt the operations of the entire P2P system.

Take the P2P video multicasting application as an example. If a malicious node joins the system using a large number of Sybil identities, the source node and the legitimate nodes in the multicast tree may accept many Sybil identities as their multicast tree children. As a result, the forwarding bandwidth of the legitimate nodes is quickly exhausted by the Sybil identities. This effectively prevents other legitimate nodes from joining the system.

As the Sybil attack is a serious threat to P2P systems, a number of Sybil attack mitigation techniques have been proposed. A review of these techniques can be found in Section 6. One technique is to use a trusted certificate authority (CA) to verify that a requester for a logical identity is a real and unique entity (e.g., a person, an organization, a CPU, etc.), and to issue cryptographically signed logical identities. If no CA is available in the P2P system, then other mitigation techniques may be used to distinguish legitimate identities and Sybil identities. The common feature among these techniques is that an identity is required to show that it is the sole owner of certain valuable things (e.g. money, an IP address, computation power, network bandwidth, trust relationships etc.).

We propose a different technique to avoid Sybil identities that is based on Internet delay space properties and assumes no CA is available. Note that the technique proposed in [2] uses network coordinates to detect Sybil identities, and at first glance, this technique may appear to be based on Internet delay space properties. However, on the contrary, it actually assumes an idealized network where delays satisfy the triangle inequality, and also assumes that a malicious node does not lie about its delays to other nodes.

1.2 Exploiting Internet Delay Space Properties

The contribution of this paper is the demonstration that the statistical properties of the Internet delay space can be used to greatly limit Sybil identities' ability to fake their network locations. The effect is that no matter how many Sybil identities a malicious node creates, with high likelihood they can only appear to originate from a small number of credible network locations. Thus, to mitigate the impact of a Sybil attack, a legitimate node can simply choose to trust identities that originate from a diverse set of network locations.

The technique exploits two properties of the Internet delay space: (1) a network location cannot have small delays to all other network locations, and (2) if the delays from a network location to other network locations have been inflated heavily, the resulting delays will have unusual statistical properties.

Furthermore, the technique uses a set of trusted distributed landmarks (such as Planetlab nodes) to measure their delays to an identity. Each identity is then assigned to the closest nearby landmark. If the delay from an identity to its closest landmark is larger than an empirically determined threshold T, then this identity is rejected since it is located in a suspicious location far from all landmarks. By property (1), Sybil identities originating from a network location can only be assigned to a small subset of landmarks whose original delays to the malicious node are less than T. This provides a coarse grained segregation of the Sybil identities from legitimate identities and limits their influence.

Furthermore, the landmark delays create a network location "fingerprint" for an identity and each fingerprint is associated with a realism measure based on the statistical properties of the landmark delays. A legitimate node only trusts identities originating from

[1]In this paper, "delay" means round-trip delay.

different network locations that have different fingerprints. Among identities with similar fingerprints, a legitimate node prefers the identity with the highest realism measure. Thus, in order to launch an effective Sybil attack, a malicious node is forced to manipulate and inflate delay measurements to create different fingerprints for different Sybil identities. However, by property (2), any significant manipulation will violate the statistical properties of the delay space. Thus, a malicious node cannot manufacture many distinct fingerprints with high realism measure. This technique therefore effectively limits the fraction of Sybil identities accepted by a legitimate node.

We conduct a measurement-based evaluation of this technique. A key result is that, assuming 100 Planetlab nodes are used as landmarks, 6,000 peers are randomly scattered over the Internet, and the malicious node is at a random network location creating over 10 million Sybil identities, this technique can limit the percentage of Sybil identities accepted by a legitimate node to below 5%.

The rest of this paper is organized as follows. We establish the important delay space properties using Internet measurements in Section 2. We present our technique and provide empirical justifications in Section 3. The technique's effectiveness and characteristics are evaluated in Section 4. We discuss several additional details in Section 5. Section 6 presents the related work, and we conclude the paper in Section 7.

2. PROPERTIES OF THE INTERNET DELAY SPACE

In order to study how the properties of the Internet delay space can be useful in mitigating the Sybil attack and evaluate our technique, we first collect Internet delay measurements using Planetlab [19]. Our data collection methodology is presented in Section 2.1. Two interesting properties of the Internet delay space that our technique relies on are introduced in Section 2.2.

2.1 Data Collection Methodology

As described in the introduction, our technique uses a set of trusted landmarks to measure other regular nodes. In our measurements, the two types of nodes are selected as follows:

Landmark selection: In our technique a set of trusted landmarks are used to probe other peers and generate fingerprints for them accordingly. We use the Planetlab testbed (consisting of 826 machines in 406 sites) as the candidate landmarks. We select one machine from each Planetlab site and then keep the 100 machines with the lightest workload. We do not use those overloaded machines because the measurements performed from them may be skewed.

Live IP addresses for simulating regular nodes: In order to choose live IP addresses to simulate nodes on the Internet, we start with a list of 20,000 random IP addresses drawn from the prefixes announced in BGP as published by the Route Views project [21]. We probe each IP address to test whether it responds to ICMP Echo Request [13], and finally we get 7,000 live IP addresses that respond to our ICMP probes. We will use these 7,000 IP addresses to simulate regular nodes in this paper. Because the IP addresses are randomly chosen, they should be able to approximate the Internet delay space.

Note that in an actual implementation, using ICMP Echo request to measure delay is only one of many options. If a node does not respond to ICMP Echo request because it is turned off or it is behind a firewall, we can use its last-hop router to represent it. Transport-level ping or application-level ping may also be used to measure delays.

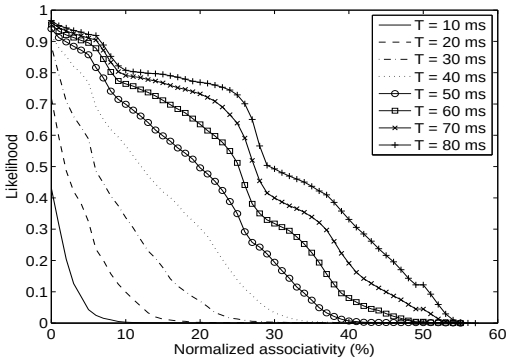

Figure 1: Associativity of network nodes with different T.

Probing: We let each selected landmark machine probe all the 7,000 live IP addresses to measure the round-trip time (RTT) between the landmarks and all IP addresses. Each IP is probed 5 times from each landmark and the minimum of the 5 delay samples is used. This produces a 100 $\times$ 7,000 delay matrix for our study. The landmarks also probe each other to measure the delays among themselves using the same probing methodology.

The following discussion about the Internet delay space properties and the empirical results presented in Section 3 and 4 are based on this data set.

2.2 Two Properties of the Internet Delay Space

Many interesting properties of the Internet delay space have been identified recently, including triangle inequality violations (TIV), constrained growth property, clustering property, etc. While these previous findings inspired our work, they however do not directly translate into useful properties for Sybil attack mitigation. Here, we establish the following two properties of the Internet delay space that our technique is based on.

• Property 1: A network location cannot have small delays to all other network locations.

This property is straightforward to see because the delay between any two network locations is ultimately lower bounded by the speed of light delay across the physical distance between the two network locations.

In order to quantify this property, we study how many landmarks one node can be close to in our data set. We define the *associativity* of one node N given an *associativity threshold* T as the number of landmarks that are within T distance to N. The *normalized associativity* is just the associativity divided by the total number of landmarks. Figure 1 shows the normalized associativity with different associativity thresholds T. As can be seen, given a reasonable T, the likelihood that one node can be associated with a large fraction of landmarks is small. For example, given $T = 30$ ms, the likelihood that a random network node can be associated with more than 30% of the landmarks is nearly zero.

• Property 2: If the delays from a network location to other network locations have been inflated heavily, the resulting delays will have unusual statistical properties.

This property can be further interpreted in two folds:

Property 2.1: Triangle inequality violations (TIV) widely exist but they happen far less frequently among nearby nodes. If a node inflates its delays to nearby nodes, it is very likely to cause unusual TIVs.

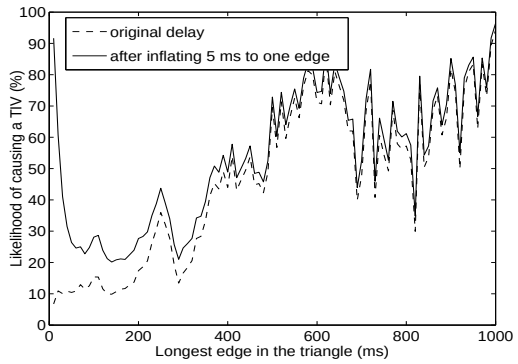

Figure 2: Likelihood of causing a TIV in one triangle with respect to the longest edge in the triangle.

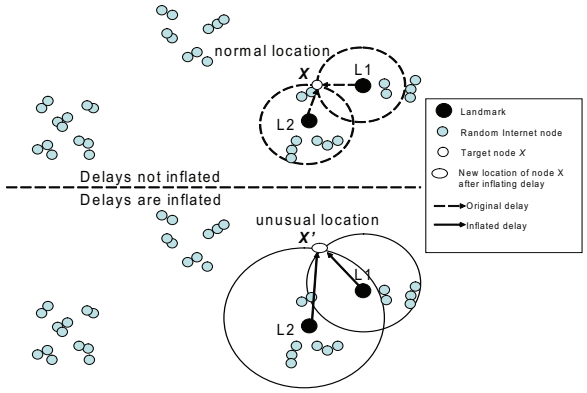

Figure 3: Nodes cannot appear in an arbitrary location in the Internet delay space: if X does not inflate delays, it should appear at a normal location clustered with other nodes; if it does inflate delays, it will appear to be located in an unusual location.

The Internet delays do not always obey the triangle inequality property because the Internet routing is not always optimal with respect to delays. Studies [25, 23] have shown that a small fraction of triangles in the Internet delay space violate triangle inequality and that long delays are more likely to cause a TIV. We have confirmed this property based on our Planetlab data set. The dotted line in Figure 2 shows the likelihood of one triangle causing a TIV with respect to the longest edge in that triangle.

The question then is, how does inflating delays change the TIV characteristics? The solid line in Figure 2 shows the likelihood that one triangle will cause a TIV if one of its edges is inflated by a small amount of delay, specifically 5 ms. As can be seen, triangles with small delays are highly sensitive to such small delay inflation, resulting in an unusually high likelihood of TIV. This result indicates that if we consider triangles with small delays, triangles with manipulated delays can be detected by inspecting their TIVs.

Property 2.2: The Internet delay space forms multi-level clusters due to the heterogeneous physical distribution of nodes. Thus, the delays among a set of nodes conform to the clustering structure and cannot be random. If a node inflates delays to other nodes arbitrarily, those delays may not conform to the characteristics of delays found in a normal delay space.

Internet hosts are not randomly distributed and thus the Internet delay space has a non-uniform structure. Studies such as [25] have shown that the continents (North America, Europe and Asia) with the largest concentration of IP subnetworks form recognizable clusters in the delay space. In addition to the global-scale clustering structure in the delay space, within each continent Internet hosts are concentrate in populated areas like big cities and form local clusters. This clustering property indicates that a node is highly unlikely to appear at an arbitrary location in the Internet delay space, i.e., it cannot have arbitrary delays to other nodes. To illustrate this property, in Figure 3, we use nodes on a 2-D plane to represent hosts in the Internet. Consider the top half of the figure. Assume node X is originally located in a local cluster and the delays from X to two landmarks L_1 and L_2 are represented by the dashed arrows. From the points of view of landmarks L_1 and L_2, node X appears to have a legitimate location because two other nodes also reside in the same neighborhood. But if X inflates its delays to landmarks L_1 and L_2 (the delays after inflation are represented by solid arrows in the bottom half of Figure 3), it will appear to have a new and unusual location X' to landmarks L_1 and L_2, where no other legitimate nodes exist.

The Internet delay space is certainly not as simple as a 2-D plane. We need to quantify whether a set of delays is normal or unusual in the delay space. Given a set of landmarks $(L_1, L_2, ..., L_n)$, the *fingerprint* of a node i is defined as the delay vector composed of delays from a number of landmarks to node i: $(d_i^1, d_i^2, ..., d_i^m)$, where $m \leq n$ and d_i^k is the delay between landmark L_k and node i. Given any two fingerprints $(d_i^1, d_i^2, ..., d_i^m)$ and $(d_j^1, d_j^2, ..., d_j^m)$ for node i and node j, the *distance between the two fingerprints* is defined as the Manhattan distance of the two fingerprints: $\sum_{k=1}^{m} |d_i^k - d_j^k|$. Furthermore, we assign a *confidence* value to each fingerprint by counting the number of fingerprints of legitimate nodes in our data set that are within certain *confidence threshold* t to this fingerprint.

Given the above definition, we randomly select three landmarks and then generate a fingerprint for each node in our data set based on the selected three landmarks, then we can calculate the confidence values of all the 7,000 fingerprints. For comparison, we also calculate the confidence values of fake fingerprints. The fake fingerprints are generated by inflating the delays in the original 7,000 fingerprints by certain random values. Figure 4 shows the comparison result using $t = 3$ms. As can be seen, the confidence values of those fake fingerprints are much lower than the legitimate fingerprints. And the more heavily the delays are inflated, the lower are their confidence values. This indicates that when a node inflates delays, it will appear to have an unusual location where few other legitimate nodes exist.

3. TECHNIQUE FOR SYBIL ATTACK MITIGATION

In the previous section, we have presented two key properties of the Internet delay space and their sensitivity to artificial delay manipulation. In this section, we present how those delay space properties can be used to mitigate a Sybil attack.

3.1 Threat Model

Our goal is to mitigate the Sybil attack originating from a particular network location. The first strawman solution is to check whether different identities share the same IP address for communications. If they do, they are definitely from the same network location and so a legitimate node can choose to avoid them. However, a malicious node may be able to hijack a large number of IP addresses [12, 1, 26] and give each Sybil identity its own unique IP address for communications. The second strawman solution is

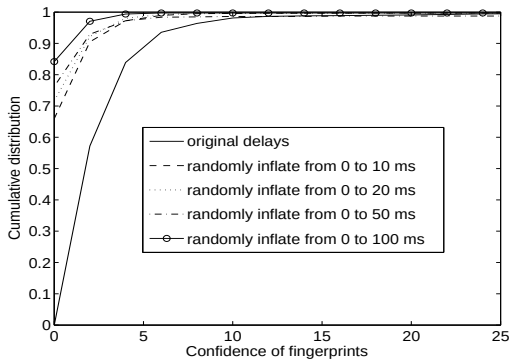

Figure 4: If nodes inflate delays randomly, their confidence measure will be very likely to be lower than those of legitimate nodes.

to use the traceroute tool to check whether different identities share the same upstream router. If so, they are definitely from the same network location. However, a malicious node may reply to traceroute messages with different fake network hops for each Sybil identity to pretend that the identities originate from different network locations. Thus, both IP address and traceroute based strawmans can be defeated by a malicious node. In general, we assume a malicious node has the following capabilities:

• It can possess an unlimited number of logical Sybil identities.

• It can hijack a large number of IP addresses and give each Sybil identity its own IP address.

• It can respond with fake network hops when a party attempts to traceroute to a Sybil identity.

• It can inflate the measured delay from a party to it arbitrarily by holding onto the delay probe message for an arbitrary amount of time. Note, however, that it is fundamentally impossible for a malicious node to reduce the measured delay.

• It knows everything about the Sybil attack mitigation strategy employed. The mitigation strategy cannot rely on obscurity.

Our proposed technique simply leverages Internet delay space properties to mitigate the Sybil attack. It is effective even if a malicious node tries to game the system by inflating measured delays arbitrarily.

3.2 Technique Overview

Our approach takes as input a list of identities, of which an arbitrary number could be Sybil identities originating from a malicious node, and then outputs a subset of carefully selected identities that minimize the fraction of Sybil identities chosen. Figure 5 illustrates the two key components in our approach: one component is used to assign a fingerprint to each identity and the other component is used for selecting a subset of identities based on their corresponding fingerprints.

Let us again take the video broadcasting application as an example to see how the proposed technique can be used. In Figure 6(a), there is no Sybil attack defense available, so when a Sybil attack is launched, the forwarding bandwidth of existing legitimate nodes $L1$, $L2$, and $L3$ are exhausted by the swarm of Sybil identities. Later when legitimate nodes $L4$ and $L5$ want to join the broadcast, they can only use some Sybil identities as their parents and may receive no video. In contrast, Figure 6(b) shows how the proposed technique can help protect legitimate identities from being duped by Sybil identities. Assume that multiple Sybil identities and $L4$ want to join the node $L2$, $L2$ will first use the "assign fingerprint"

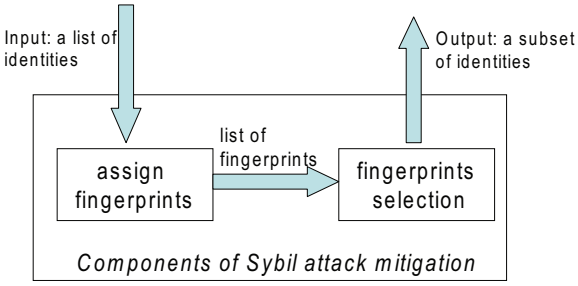

Figure 5: Two components of our mitigation technique.

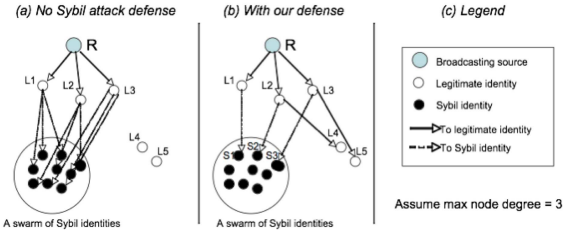

Figure 6: Sybil attack in the P2P video broadcasting system

component to assign a fingerprint to each identity, then it feeds all fingerprints to the "fingerprint selection" component. Most Sybil identities will be eliminated by the proposed technique. It is possible that a small number of Sybil identities (e.g. $S2$) from the swarm is accepted by $L2$, but $L2$ still has forwarding bandwidth left to accept $L4$ as a child. Other legitimate identities $L1$ and $L3$ are also protected similarly.

3.2.1 Landmark Initialization

When the system starts, a list of all landmarks and a list of random live IP addresses are input to each landmark. Each landmark then measures its delays to all the other landmarks and the provided random IP addresses. By probing other landmarks, a landmark will know which other landmarks are close to it. By measuring the delays from itself to the list of random IP addresses, each landmark will get an empirical sample of the Internet delay space from its own point of view. We assume the random IP addresses do not behave maliciously and simply respond to ICMP pings. Landmarks may share their measured delays with each other if necessary. In our algorithm, one landmark will request the measured delays from a number of other closest landmarks. Each landmark may periodically restart the measurements to update the measurements. We will explain how this information is used in our technique in the following.

3.2.2 Assigning Fingerprints to Identities

Assume N landmarks $(L_1, L_2, ..., L_N)$ exist in the system. The following steps are used to generate a fingerprint for an identity i.

• **Step 1:** All landmarks will probe the identity i to determine the closest landmark L_k to i.

• **Step 2:** Landmark L_k and its two closest landmarks L_m and L_n then generate a fingerprint fp_i for identity i in the format of $< (L_k, d_i^k), (L_m, d_i^m), (L_n, d_i^n) >$, where d_i^k is the measured delay from landmark L_k to identity i.

• **Step 3:** The three landmarks then calculate the confidence value $conf_i$ of the fingerprint fp_i by counting the number of legitimate fingerprints (corresponding to the random IP addresses provided to the landmarks in the initialization stage) that are within a certain

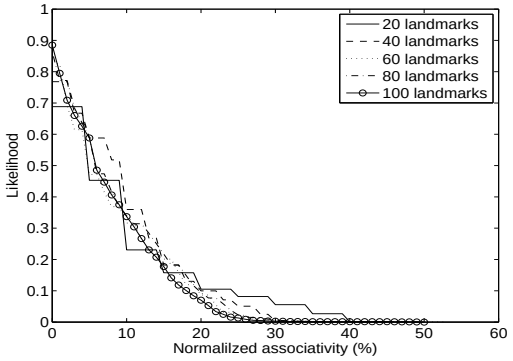

Figure 7: Associativity of network nodes with different number of landmarks.

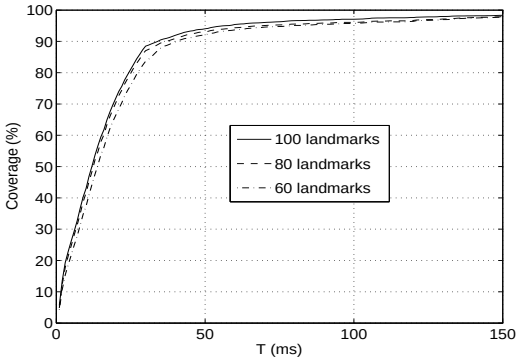

Figure 8: Coverage rate of network nodes.

confidence threshold t to fp_i. The confidence calculation is the same as explained in Section 2.2.

• **Step 4:** Since landmarks L_k, L_m and L_n know the delays among them and the delays from them to identity i, they can calculate whether i causes a TIV together with the landmarks and record this using an indicator tiv_i, where $tiv_i = 1$ means that i causes at least one TIV and $tiv_i = 0$ means that it does not cause any TIVs.

This component outputs the following information for identity i to the identity-selection component: $< fp_i, tiv_i, conf_i >$.

3.2.3 Selecting Identities Based on Their Fingerprints

Given a set of fingerprints and their corresponding TIV measure and confidence measure, this component will select a subset of fingerprints using the following rules. The reasoning behind these rules are explained in Section 3.3.

Note that these basic rules may reject a legitimate identity, resulting in a false positive. Coping with false positives is discussed in Section 5.

• **Rule 1:** If an identity causes TIVs, then we reject it.

• **Rule 2:** If the delay from an identity to its closest landmark is larger than a certain associativity threshold T, then we reject this identity because it is unacceptably far from its closest landmark. We now can classify the remaining fingerprints into different clusters based on their closest landmark. That is, fingerprints that have the same closest landmark will be classified into the same cluster. Then we can select fingerprints separately from each cluster.

• **Rule 3:** Within each cluster, we will first select fingerprints with the highest confidence measure because a fingerprint with a high confidence is considered to come from a realistic network location and is unlikely to have been manipulated. After selecting the fingerprint with the highest confidence measure, we will eliminate all other fingerprints from this cluster whose distances to the chosen fingerprint are smaller than the confidence threshold t. This is because we consider such similar fingerprints as originating from the same network location.

By using the above rules, we can select identities from the clusters in a round-robin fashion until all clusters have no more identities left. In summary, we use four techniques to defend against Sybil identities: 1) classify each identity to a local cluster, 2) favor identities not causing TIV, 3) favor identities with higher confidence, and 4) do not accept identities with similar fingerprint. The first three techniques are direct applications of the Internet delay space properties.

3.3 Exploiting Delay Space Properties for Sybil Attack Mitigation

In this section, we explain in detail how the above defense techniques effectively exploit the properties of the Internet delay space.

• **Exploiting Property 1:** Each identity is first associated with its closest landmark given a certain associativity threshold T. Identities associated with a particular landmark form a cluster.

A legitimate identity will simply be associated with its closest landmarks within delay T. A malicious node, however, will try to associate the Sybil identities it generates with as many landmarks as possible by manipulating the delays to make different Sybil identities appear closest to different landmarks.

However, property 1 guarantees that Sybil identities from a malicious node can only be present in a small fraction of clusters because the malicious node has limited associativity. As a result, if identities are chosen among clusters in a round-robin fashion, the fraction of Sybil identities chosen can be bounded by the associativity of the malicious node.

Figure 7 shows that when the number of landmarks changes, the normalized associativity of network nodes is quite stable (associativity threshold is 30ms). In other words, it is not very sensitive to the number of landmarks used. Moreover, the likelihood that a network node can be associated with a large fraction of landmarks remain small. When 100 landmarks are used, nearly no node can be associated with more than 30% of the landmarks. Thus, a malicious node and all Sybil identities it creates cannot be associated with more than 30% of the landmarks.

Obviously, the associativity of a node varies with the associativity threshold T. Referring to Figure 1 again, it shows that as T increases, a node (and thus all Sybil identities it may originate) can associate with a larger fraction of landmarks. Thus, the goal is to choose a small enough T such that a node cannot be associated with many landmarks, and at the same time most nodes can associate with at least one landmark.

Figure 8 shows how many nodes can be associated to at least one landmark with varying number of landmarks and associativity threshold T. As can be seen, given a reasonable threshold T, e.g., 30 ms, about 90% of nodes can be associated to a landmark. We can also see that a small fraction of nodes cannot be associated with any landmark even if we use a relatively large T. We find that these nodes usually come from countries where no Planetlab nodes exist. Thus, in order to cover these nodes with a reasonably small T, a more diverse set of landmark locations are necessary.

In summary, if we use a reasonably small T, e.g., 30 ms, then about 90% of legitimate nodes can be associated with their closest

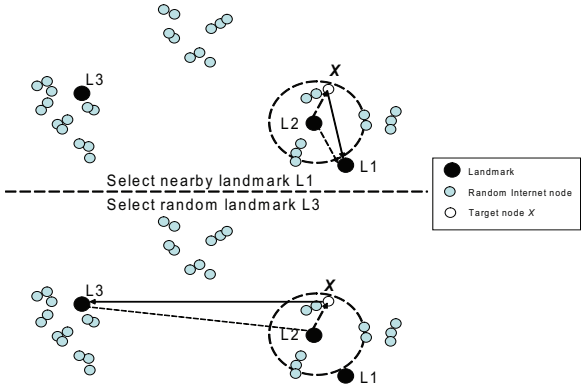

Figure 9: Illustration of using nearby landmarks to assign fingerprint.

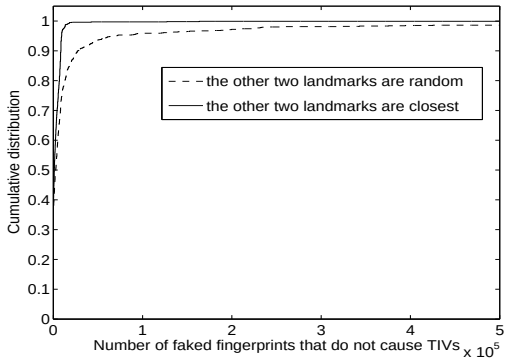

Figure 10: Cumulative distribution of number of fake fingerprints that do not cause TIVs for all possible network locations in our data set.

landmarks while Sybil identities originating from a malicious node can only manage to associate with a small fraction of landmarks.

• **Exploiting Property 2.1:** Property 2.1 states that TIVs happen less often among nearby nodes and if a node inflates delays to nearby nodes, it is likely to cause unusual TIVs. This property explains why we need to use a node i's closest landmark L_k and L_k's two closest landmarks L_m and L_n to generate a fingerprint for node i. By using nearby landmarks to generate fingerprints we can reduce the number of legitimate nodes that are falsely rejected by applying Rule 1 and have a better chance to detect the manipulated delays by a malicious node. Figure 9 uses a simple example to demonstrate this property. In Figure 9, node X's closest landmark is L_2. If we use a nearby landmark L_1 together with L_2 to generate a fingerprint for X, then X cannot inflate its delay to L_1 too much because the other two edges L_1L_2 and L_2X are already short. On the other hand, if the landmark L_3 is used to generate a fingerprint for node i, then because the edge L_3L_2 is relatively long, a malicious node can inflate the edge L_3X a lot without causing a TIV.

Experiments show that if nearby landmarks are used to generate a fingerprint for each legitimate node, 16.2% of legitimate nodes will be falsely rejected because of them causing TIVs. In contrast, if random landmarks are used to generate fingerprints for legitimate nodes, 33.9% of legitimate nodes will be falsely rejected. Therefore using nearby landmarks can greatly reduce the negative impact on legitimate nodes. Further discussion on coping with false positives can be found in Section 5. In addition, using nearby landmarks to generate fingerprints also helps to limit the total number of possible fake fingerprints. We generate fake fingerprints for each node in our data set in this way: given a node i and three landmarks including its closest landmark, we generate all possible fingerprints by inflating the delay to its closest landmark in 1 ms increments, up to the associativity threshold T and inflating its delays to other two landmarks in 1 ms increments until the inflated delays cause TIVs. Figure 10 compares the number of possible fake fingerprints by using nearby landmarks and using random landmarks. The result shows that if random landmarks are used, a malicious node can generate a lot more fake fingerprints compared with using nearby landmarks.

• **Exploiting Property 2.2:** Property 2.2 states that when a node inflates delays heavily, it will appear to be at an unusual location. Our technique uses the confidence measure of a node's fingerprint to measure whether it resides at a realistic location. In order to compare the confidence values of legitimate fingerprints and fake fingerprints, we first calculate the confidence values for all legitimate fingerprints in our data. Then we calculate the confidence values of all possible fake fingerprints. Note that we use nearby landmarks to generate fingerprints. Figure 11 compares the confidence values of legitimate fingerprints and fake fingerprints. It shows that fake fingerprints have much lower confidence measure than legitimate fingerprints.

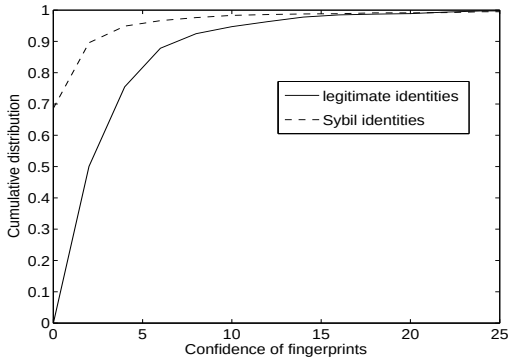

Figure 11: Confidence comparison of legitimate fingerprints and Sybil fingerprints.

4. EVALUATION

In this section, we evaluate the overall effectiveness of our technique. A *reference delay space* is needed by the landmarks for each experiment in this section. The reference delay space is composed of delays from all landmarks to a subset of the random IP addresses. Landmarks will use the reference delay space to calculate the confidence values for all legitimate identities and Sybil identities. The remaining random IP addresses then can be used to simulate legitimate network locations in the system. Note that the IP addresses used in the reference delay space and the IP addresses used to represent legitimate network locations are disjoint. In this section, unless otherwise stated, the associativity threshold T is 30 ms, the confidence threshold t is 3 ms, the number of landmarks used is 100.

When one malicious node takes control of a network location, we assume it can selectively inflate delays to get associated with all the landmarks that are within T delay to it instead of always associating with the true closest landmark. We name those land-

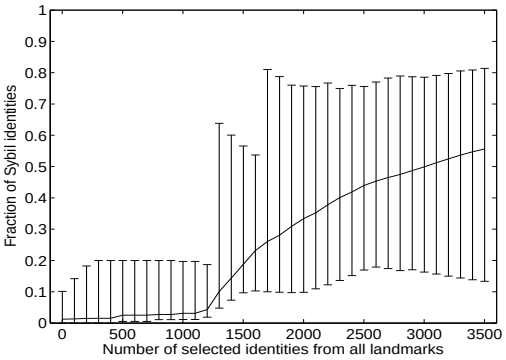

Figure 12: Fraction of Sybil identities from all landmarks.

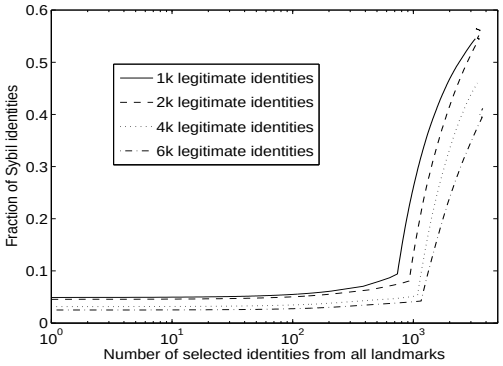

Figure 13: Fraction of Sybil identities from all landmarks.

marks that are within T distance to the malicious node as *vulnerable landmarks* because they can be affected by the malicious node. The behavior of the malicious node is then: for each vulnerable landmark, the malicious node will generate as many Sybil identities as possible by inflating all possible delays in 1 ms increments to the corresponding landmarks to create fake fingerprints and then let those Sybil identities join the system. The number of faked fingerprints a malicious node can create varies according to the exact location of the malicious node, but on average it can create over 13 million Sybil identities associated with all possible vulnerable landmarks. We always let all legitimate identities join the system. Then the identity selection component is used to select a subset of identities out of all those legitimate identities and Sybil identities. We want to study how well we can limit the fraction of Sybil identities selected using our technique.

4.1 Basic Performance

In this section, we first fix the size of the reference delay space and the number of legitimate locations at both 3500 to show the basic performance of our technique. We let the malicious node take control of one network location in each experiment. The experiment is repeated for all possible network locations. The results presented here are accumulated over all possible network locations. If we select identities from all available landmarks in a round-robin fashion, Figure 12 shows the average fraction of accepted Sybil identities with 10% and 90% error bar. As can be seen, if the number of selected identities is below 1000, then the fraction of selected Sybil identities in most cases is below 5%. When we select more and more identities, legitimate identities will be exhausted sooner or later. When all the non-vulnerable landmarks are exhausted, the fraction of selected Sybil identities will increase sharply because vulnerable landmarks are still feeding Sybil identities.

Although the above experiment has demonstrated the effectiveness of using the proposed technique to mitigate the Sybil attack, the next natural question is how the performance of the technique will change with the increase of the number of legitimate locations. In our second experiment, we fix the size of the reference delay space at 1000 nodes, then we vary the number of legitimate locations from 1000 to 6000. Figure 13 shows the average fraction of selected Sybil identities. As can be seen, when we increase the number of legitimate locations, although the maximum number of legitimate locations (i.e., 6000) is still only about 0.05% of the total number of created Sybil identities (13 million), the performance of the technique is improved because more legitimate identities are competing with Sybil identities.

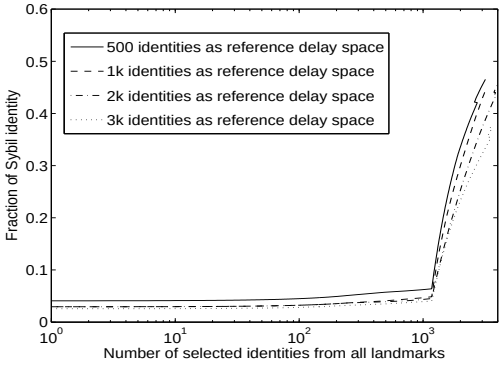

Figure 14: Fraction of Sybil identities from all landmarks.

4.2 Impact of Size of Reference Delay Space

In this experiment, we fix the number of the legitimate locations at 4000. Then we vary the size of reference delay space from 500 to 3000. Figure 14 shows the average fraction of selected Sybil identities. We can observe that generally the larger the reference delay space, the better the performance. We can also observe that the benefit of increasing the size of the reference delay space diminishes. The performance of using a 1000-node reference delay space is very close to the performance of using a 3000-node reference delay space. This indicates that even if the landmark only probes 1000 IP addresses on the Internet, it still can provide good performance. Thus, the overhead of constructing a sufficient reference delay space is reasonably low.

4.3 Performance Sensitivity to Parameters

Three configurable parameters are used in our technique: the number of landmarks, the associativity threshold T and confidence threshold t. All experiments in this section use 3500 nodes as the reference delay space and use the other 3500 nodes as the legitimate nodes in the system.

We first study the performance of our technique using different number of landmarks. We use $T = 30$ ms and $t = 3$ ms, then we vary the number of landmarks from 20 to 100. Figure 15 shows the average fraction of selected Sybil identities. As can be observed, when we only select a small number of identities, the performance of using different number of landmarks does not differ too much; but when we select more and more identities, the performance of using fewer landmarks becomes worse sooner. This

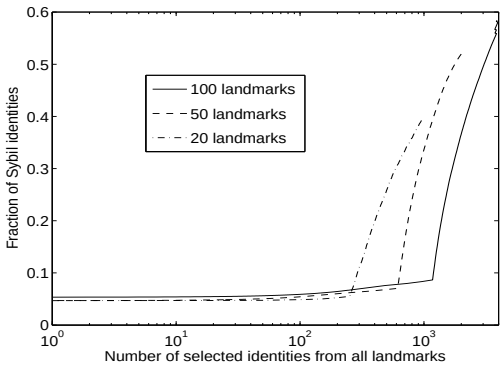

Figure 15: Fraction of Sybil identities from all landmarks.

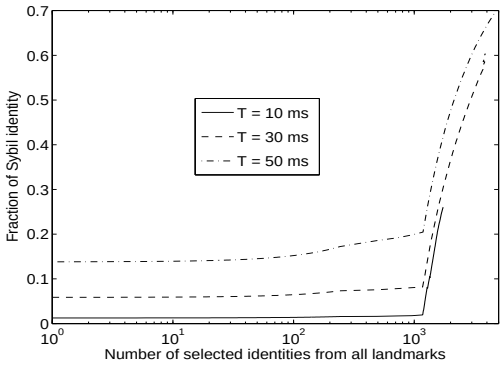

Figure 16: Fraction of Sybil identities from all landmarks.

is because by using fewer landmarks, we cover fewer legitimate identities. Thus, when we select more and more identities, the non-vulnerable landmarks are exhausted quicker when there are fewer landmarks. However, before the non-vulnerable landmarks are exhausted, the technique can effectively limit the fraction of selected Sybil identities even when a small number of landmarks (e.g., 20) are used.

Next, we study how the associativity threshold T affects the performance of our technique. We use 100 landmarks and $t = 3$ ms, then vary T from 10 ms to 50 ms. Figure 16 presents the average fraction of selected Sybil identities. As can be seen, when a smaller T is used, the fraction of Sybil identities selected also becomes smaller. This is because when a smaller T is used, a malicious node can be associated with a smaller fraction of landmarks as shown in Figure 1. The problem of using a small T is that many legitimate nodes will not be able to associate with any landmark. At $T = 10$ ms, 57% of nodes cannot associate with any landmark. By using a larger T, more nodes will be able to associate with some landmarks, but correspondingly the malicious node can also manage to associate with more landmarks, which is not desirable.

Finally, we study how the confidence threshold t affects the performance of our technique. We use 100 landmarks and $T = 30$ ms, then we vary t from 1 ms to 5 ms. Figure 17 shows the average fraction of selected Sybil identities. As can be seen from the graph, when a larger t is used, the fraction of Sybil identities selected is smaller. The reason is that a larger t will cause more Sybil identities to get eliminated when we select one identity.

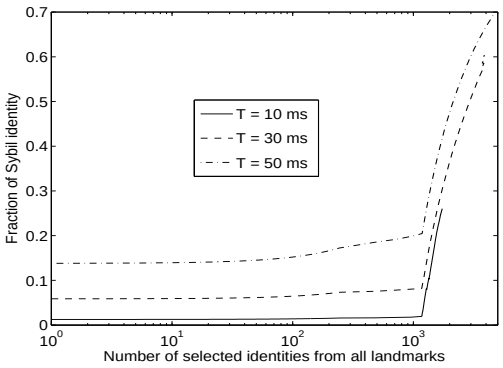

Figure 17: Fraction of Sybil identities from all landmarks.

5. DISCUSSION

Although the proposed technique is effective in mitigating a Sybil attack, it incurs certain overheads and thus should only be used when necessary. Each application should decide when it is appropriate to use the technique. For example, in the video broadcasting application, when a node's remaining forwarding bandwidth is high, this technique is not needed. However, when a node receives an unusually high number of join requests or when it is running out of forwarding bandwidth, these may be signs that the node is under a Sybil attack. The node can start using the technique to perform a more careful peer selection.

A Sybil attack usually involves a huge number of Sybil identities. In our experiments, we have created as many as 13 million Sybil identities in a single attack. It is not possible for a statistical technique to perfectly distinguish a much smaller number of legitimate identities from such a huge number of Sybil identities. Some false positives and some false negatives must be accepted as a consequence. The false negative rate of our technique is low as the fraction of Sybil identities selected is below 5%. Two kinds of false positive may occur: *system-wide false positive* and *node-specific false positive*. For example, if a legitimate node A is not selected by node B because A is too far from all landmarks, then it is a *system-wide false positive* since A cannot be selected by any node in the system. Legitimate nodes that suffer from system-wide false positive are sacrificed. On the other hand, if legitimate node A is not selected by node B because of another competing node C that has a similar fingerprint to A but a higher confidence, then it is a *node-specific false positive* since A can still try to join nodes other than B.

As an example of the *node-specific false positive*, a node cannot pick two other nodes that reside in one physical LAN because they have similar fingerprints, even though they are both legitimate. This restriction is acceptable to most applications due to two reasons. Firstly, two nodes in the same LAN can still participate in the P2P system at the same time although they cannot be both selected by the same node. Examples of this are shown in Figure 18. In Figure 18(a), $L1$ and $L2$ pick $L6$ and $L7$ as their child respectively, although $L6$ and $L7$ cannot be picked by either $L1$ or $L2$ at the same time. In Figure 18(b), $L1$ picks $L6$ as its child and then $L6$ picks $L7$ as its child. In both cases, all the nodes can still participate in the system. Secondly, peer location diversity is a desirable property to most applications as it enhances the robustness of a P2P system. Imagine a legitimate node whose peers are all inside one LAN. A single failure of that LAN can disconnect the node from all its peers. On the other hand, if peers are chosen from diverse

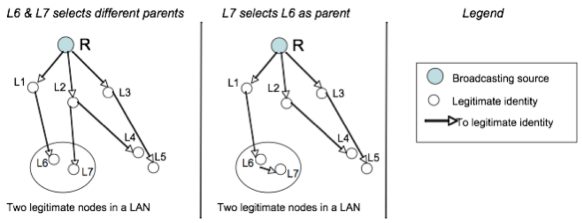

Figure 18: Multiples nodes from the same LAN

network locations, then the P2P system is also more robust against router and link failures. Unfortunately, if a node *must* use multiple identities from the same network location in order to function correctly, then the proposed Sybil attack mitigation technique will not apply.

The proposed technique requires a node to be associated with a nearby landmark. One concern is whether the technique discriminates against nodes with big last-hop delays caused by the access network such as cable modem and DSL. Actually, for a node with a big last-hop delay, we may use its last-hop router to represent it. That is, we can assign the fingerprint of the node's last-hop router to it. A recent study [7] shows that last-hop routers of residential broadband nodes have much smaller delays to other nodes in the Internet. It is important to note that using the fingerprint of the node's last-hop router does not reduce the effectiveness of our technique because it does not give a malicious node any more power to fake network locations.

In its basic form, our technique requires the landmarks to be trusted. However, what if one or more landmarks are compromised? What are the effects? Is there any remedy? If a landmark is compromised, it can report arbitrary delays to both legitimate and Sybil identities, which can affect the system badly. For example, by reporting very small delays to legitimate identities, a compromised landmark can claim itself to be the closest landmark to them. This can cause legitimate identities to violate the triangle inequality. Additionally, the compromised landmark can help the Sybil identities to obtain more realistic delay fingerprints. If more than one landmarks are compromised, then they can also collude. For example, the compromised landmarks can fake the delays among themselves so that they can act as each other's nearby landmarks. Two compromised landmarks are enough to fail a legitimate identity by creating a TIV. Three colluding compromised landmarks can fake arbitrary fingerprints for any nodes. In order to detect such compromised landmarks, landmarks can audit each other. For example, if a legitimate landmark detects that another nearby landmark reports small delays to some nodes that are far to itself, then it has a reason to believe that the nearby landmark is lying. This kind of auditing mechanism can help make our approach more secure, but designing such mechanisms is beyond the scope of this paper.

Another landmark related concern is scalability. The landmarks could be overwhelmed by the measurement requests from either legitimate or Sybil identities. The scalability problem can be alleviated if certain mechanisms are employed to reduce the measurement overhead. For example, each landmark can cache the measured delays for a certain amount of time so they can be reused later. If the system is only consisted of legitimate identities, the caching mechanism can help improve the scalability by reducing the active measurements. However, if malicious nodes exist, they can keep creating new Sybil identities and requesting fingerprints for them. In order to defend against such kind of DoS attack, the landmarks have to use certain rate limiting mechanism.

Another issue is, will the Internet delay space properties required by our technique be stable over time? First, it should be clear that because of the speed-of-light delay lower bound, Property 1 is always true. We argue that Property 2 should also remain true. Triangle inequality violation in the Internet delay space is caused by the routing policy of the Internet. While the routing policy may evolve over time, the amount of triangle inequality violation should not dramatically increase since ISPs have strong incentives to provide customers with low end-to-end delay. In addition, the distribution of nodes in the Internet is highly likely to remain very heterogeneous and clustered. Areas where few people live and where the ocean covers will most likely have very few nodes. Thus, a manipulated fingerprint is still likely to appear unusual for the foreseeable future.

Malicious attackers are becoming ever more sophisticated. Botnets [5, 20] are a serious threat to the security of P2P systems. What if an attacker launches the Sybil attack from a large number of physically distributed locations using a botnet? In this case, other complementary defense techniques such as social network based defense [24] and Botnet defense [11] should be used in conjunction. And despite the use of a botnet, our proposed Sybil attack mitigation technique can still help limit each zombie node to only create a small number of Sybil identities with realistic fingerprints.

6. RELATED WORK

Douceur [8] first proposed the concept of Sybil attack and proved that without a trusted certificate authority (CA), Sybil attack is always possible except under extreme and unrealistic assumptions. After this first investigation on Sybil attack, various Sybil attack mitigation techniques have been studied.

Many researchers [3, 8] have recommended the CA based Sybil attack mitigation technique. In this technique, a trusted CA that issues and verifies credentials unique to an actual node is used to defend against the Sybil attack. For example, if a P2P system requires each node to register with some sensitive information such as a legal social security number or passport number, it will make Sybil attacks much harder to be launched. Unfortunately, there are many scenarios where CA-based solution is neither available nor desirable.

If no CA is available in the P2P system, then other mitigation techniques may be used to distinguish legitimate identities and Sybil identities. Checking the distinctness of IP addresses is the most prevalent Sybil attack mitigation technique nowadays. Many systems, e.g., [10], specifically test for IP addresses distinctness to mitigate the Sybil attack. The IP-based technique relies on the assumption that one node has only one IP address. However the assumption does not always hold since a malicious node can steal multiple IP addresses from the local network. In addition, IP harvesting and IP prefix hijacking [12, 1, 26] make the situation even worse. So using IP address as the sole identity cannot solve the Sybil attack problem.

SybilGuard [24] uses the trust relations (e.g, friend relations) in the real world to detect Sybil attack and it relies on the assumption that it is hard for malicious nodes to obtain trust relations from real entities. SybilGuard tries to leverage the fact that malicious nodes can create many Sybil identities but they can only build very few trust relationships. SybilGuard uses social network and a random walk algorithm to detect multiple Sybil identities that belong to the same malicious node. SybilGuard can work well if there exists a secure social network. However the social network required in this approach is not always available in a P2P system.

Bazzi and Konjevad [2] propose to use network coordinates [18, 6] as the location certificates of nodes to mitigate Sybil attack. [2]

uses a set of beacons to probe each node and then computes a coordinate for it. This technique relies on the assumption that the Internet delay space conforms to the metric properties (symmetry, definiteness, triangle inequality), so each node can be assigned a secure coordinate by measuring its distances to a set of beacons. However, the assumed metric properties do not hold for real Internet delay space. In addition, the network coordinates still cannot be secured by current techniques.

Another class of techniques requires each node to pay something like money or CPU time to get one ID, so it will certainly increase the barrier for a malicious node to launch a Sybil attack because the resources under its control is limited, although at the same time it may also scare away many legitimate nodes. [22] propose an admission control system that mitigates Sybil attacks by adaptively constructing a hierarchy of cooperative admission control nodes. This scheme tries to prevent the malicious node from obtaining a large percentage of identities in the system very quickly, but powerful attackers with rich computation resources can still win. And eventually if the malicious nodes are given enough time they will still obtain a large fraction of identities in the system.

In addition to the work exploiting Sybil attack mitigation techniques in P2P systems, [17] studies the Sybil attack problem in sensor networks. Some mitigation techniques such as radio resource testing and random key pre-distribution are proposed. However those techniques are specific to sensor network applications and cannot be applied directly to Internet-scale decentralized systems like P2P systems.

Sybil attacks also often happen in reputation systems (e.g., user's rating on eBay), where the malicious user creates many Sybil identities to boost the rating of a certain user. A number of mitigation techniques [9, 4] have been proposed. Unfortunately the Sybil attack problem in reputation systems is fundamentally different from the case in P2P system so those mitigation techniques cannot be applied to our case directly.

7. CONCLUSIONS

The contribution of this paper is that we have shown how Internet delay space properties can be exploited to greatly limit Sybil identities' ability to fake their network locations, and how this can be used to mitigate the Sybil attack problem. It is somewhat surprising to see that the simple delay space properties examined in this paper, when applied strategically, can lead to an effective Sybil attack mitigation technique. This new technique provides an additional weapon against the challenging Sybil attack problem.

8. REFERENCES

[1] Hitesh Ballani, Paul Francis, and Xinyang Zhang. A study of prefix hijacking and interception in the internet. In *ACM SIGCOMM*, August 2007.

[2] R. Bazzi and G. Konjevod. On the establishment of distinct identities in overlay networks. In *ACM PODC*, July 2005.

[3] M. Castro, P. Druschel, A. Ganesh, A. Rowstron, and Dan Wallach. Secure routing for structured peer-to-peer overlay networks. In *ACM OSDI*, December 2002.

[4] A. Cheng and E. Friedman. Sybilproof reputation mechanisms. In *ACM SIGCOMM Workshop on Ecnomics of Peer-to-Peer Systems*, 2005.

[5] E. Cooke, F. Jahanian, and D. McPherson. The zombie roundup: Understanding, detecting, and disturbing botnets. In *Proceedings of the First Workshop on Steps to Reducing Unwanted Traffic on the Internet*, July 2005.

[6] F. Dabek, R. Cox, F. Kaashoek, and R. Morris. Vivaldi: A decentralized network coordinate system. In *Proceeding of ACM SIGCOMM*, August 2004.

[7] Marcel Dischinger, Andreas Haeberlen, Krishna P. Gummadi, and Stefan Saroiu. Characterizing residential broadband networks. In *ACM IMC*, October 2007.

[8] John Douceur. The sybil attack. In *IPTPS*, July 2002.

[9] M. Feldman, K. Lai, I. Stoica, and J. Chuang. Robust incentive techniques for peer-to-peer networks. In *ACM Electronic Commerce*, 2004.

[10] M. J. Freedman and Robert Morris. Tarzan: A peer-to-peer anonymizing network layer. In *ACM CCS*, November 2002.

[11] Honeynet project and research alliance. know your enemy: Tracking botnets. http://www.honeynet.org/papers/bots/.

[12] Xin Hu and Morley Mao. Accurate real-time identification of ip prefix hijacking. In *IEEE Symposium on Security and Privacy*, May 2007.

[13] Internet control message protocol. http://www.faqs.org/rfcs/rfc792.html.

[14] Sanghwan Lee, Zhi-Li Zhang, Sambit Sahu, and Debanjan Saha. On suitability of euclidean embedding of internet hosts. In *ACM SIGMETRICS*, June 2006.

[15] Eng Keong Lua and Timothy Griffin. Embeddable overlay networks. In *IEEE ISCC*, July 2007.

[16] Cristian Lumezanu, Dave Levin, and Neil Spring. Peerwise discovery and negotiation of faster paths. In *ACM HotNets*, November 2007.

[17] James Newsome, Elaine Shi, Dawn Song, and Adrian Perrig. The sybil attack in sensor networks: Analysis and defenses. In *IEEE IPSN*, April 2004.

[18] T. S. E. Ng and H. Zhang. Predicting Internet networking distance with coordinates-based approaches. In *Proceedings of IEEE INFOCOM*, June 2002.

[19] PlanetLab. http://www.planet-lab.org.

[20] Moheeb Abu Rajab, Jay Zarfoss, Fabian Monrose, and Andreas Terzis. A multifaceted approach to understanding the botnet phenomenon. In *ACM IMC*, October 2006.

[21] Route views. http://www.routeviews.org/.

[22] Hosam Rowaihy, William Enck, Patrick McDaniel, and Tom La Porta. Limiting sybil attacks in structured peer-to-peer networks. In *IEEE INFOCOM*, May 2007.

[23] Guohui Wang, Bo Zhang, and T. S. Eugene Ng. Towards network triangle inequality violation aware distributed systems. In *ACM IMC*, October 2007.

[24] H. Yu, M. Kaminsky, P. Gibbons, and A. Flaxman. Sybilguard: Defending against sybil attacks via social networks. In *ACM SIGCOMM*, September 2006.

[25] Bo Zhang, T. S. Eugene Ng, Animesh Nandi, Rudolf Riedi, Peter Druschel, and Guohui Wang. Measurement-based analysis, modeling, and synthesis of the internet delay space. In *ACM IMC*, October 2006.

[26] Changxi Zheng, Lusheng Ji, Dan Pei, Jia Wang, and Paul Francis. A light-weight distributed scheme for detecting ip prefix hijacks in realtime. In *ACM SIGCOMM*, August 2007.