Citation Evidence Report

EB-2 NIW Petition — National Interest Waiver

Matter of Dhanasar · Prong 2 (well-positioned)

Robert Beverly

Professor of Computer Science, San Diego State University

Google Scholar profile

Generated 2026-05-21 by CiteMap. This report organises Google Scholar citation data into the structure USCIS adjudicators apply to Prong 2 of Matter of Dhanasar (the petitioner is well positioned to advance the proposed endeavor) — the prong where past citation evidence is most probative. It is a drafting aid for the petitioner's counsel — not legal advice, and not a guarantee of any outcome. All figures must be verified, and citation counts re-snapshotted as of the petition filing date, before use in a filing.

A. Overview & Filtering Statement

46	46	5	33
Citing papers mapped	Citation edges	Home papers mapped	h-index (GS)

Filtering statement — methodology & limits

Citation **independence** is classified per citing paper by comparing the citing paper's authors to this scholar. *Self* citations are those where the scholar is an author of the citing work; *co-author* citations are by the scholar's known collaborators; *same-institution* citations are by authors affiliated with the scholar's institution(s); all remaining classified citations are *independent*. Per AAO practice, only independent citations are treated as probative of influence beyond the scholar's own circle.

Known limitations — counsel must verify. (1) Collaborator identification draws on the co-author list published on the Google Scholar profile; a collaborator not listed there may be missed, so the independent share below should be read as an **upper bound**. (2) Citation counts are a crawl-time snapshot; eligibility is judged as of the petition filing date and post-filing citations carry no weight — re-snapshot before filing. (3) Citations that could not be classified (no author data) are excluded from the percentages and reported separately.

B. Citation Independence

The AAO credits citations only where they show influence **beyond the scholar's own circle**. Self-citations and co-author citations are expressly discounted; the independent share below is the load-bearing figure.

87.0% independent of 46 classified citing papers

Citation type	Count
Independent	40
Self-citation	3
Co-author	3
Same-institution	0

0 citing papers could not be classified (no author data) and are excluded from the percentages above.

C. Significant Contributions & Their Citation Evidence

Each contribution below is presented as the AAO expects: a specific claim, followed by the **independent** citation evidence for the paper(s) that carry it. Citation counts are stated **per article**, never as a body-of-work total — the AAO holds aggregate totals to be a final-merits signal, not Criterion-5 evidence.

Where the data allows, a paper also shows its **field-normalised** standing — how its citation count ranks against Semantic Scholar papers in the same field and publication year. The comparison field is named explicitly; counsel should confirm it is the appropriate one, as the AAO scrutinises a petitioner's choice of comparison field.

Contribution 1

Claim — Contribution 1

The researcher pioneered empirical methods for measuring Internet source address filtering and analyzed the economic and regulatory incentives driving the deployment of source address validation.

The researcher established a foundational line of inquiry into Internet security hygiene, anchored by the seminal 2005 USENIX workshop paper 'The Spoofer Project.' This work appears to have introduced novel techniques for inferring the extent of source address filtering across the global Internet, addressing a critical gap in understanding how effectively networks mitigate spoofed traffic. The titles suggest a methodological contribution that enabled the quantification of a previously opaque security posture.

Building on this empirical foundation, the researcher expanded the scope of this work in a 2019 publication that examines the broader ecosystem of network hygiene. By shifting focus to incentives and regulation, this follow-up paper suggests a comprehensive analysis of why source address validation is deployed—or not—linking technical capabilities to economic and policy drivers. This chronological progression indicates a deepening of the original technical contribution into a holistic study of Internet governance and security deployment.

The significance of this body of work is evidenced by its sustained impact and broad adoption within the research community. The core paper has accumulated 195 citations, while the follow-up study has garnered 146 citations, indicating enduring relevance. Notably, 91.3% of the classified citations originate from independent researchers, demonstrating that this line of work has served as a key reference point for scholars outside the researcher's immediate circle, thereby validating its independent influence on the field.

INDEPENDENT CITATIONS FOR THIS CONTRIBUTION: 14

CORE PAPER

The Spoofer Project: Inferring the Extent of Internet Source Address Filtering on the Internet

2005 · USENIX Steps to Reducing Unwanted Traffic on the Internet Workshop (SRUTI 05) · 195 citations (GS)

No.	Citing paper	Citing institution(s)	Country	S2
1	Accountable Internet Protocol (AIP) (2008)	Carnegie Mellon University, Georgia Institute of Technology, ICSI & HIIT	United States	—
2	StackPi: New Packet Marking and Filtering Mechanisms for DDoS and IP Spoofing Defense (2006)	Carnegie Mellon University	United States	—
3	Passport: Secure and Adoptable Source Authentication (2008)	University of California, Irvine	United States	—
4	TVA: A DoS-limiting network architecture (2008)	University of California, Irvine, University of Washington	United States	—
5	Real time DDoS detection using fuzzy estimators (2012)	Democritus University of Thrace	Greece	—
6	Controlling IP Spoofing through Interdomain Packet Filters (2008)	Florida State University	—	—
7	An Inter-Domain Collaboration Scheme to Remedy DDoS Attacks in Computer Networks (2018)	Lancaster University, University of Glasgow	United Kingdom	—

Independent citing papers only; self- and co-author citations excluded. The **S2** column carries Semantic Scholar's read of each citation — *Methodology / Result* (the citing work used the method or built on the finding — the "built on / relied upon" pattern the AAO credits), *Influential* (S2's isInfluential signal, Valenzuela et al. 2015), or *Background* (a passing mention).

FOLLOW-UP WORK

Network hygiene, incentives, and regulation: deployment of source address validation in the internet

2019 · 146 citations (GS)

Field-normalised: 89 Semantic Scholar citations place it in the top 10% of Computer Science papers from 2019 indexed by Semantic Scholar, by citation count.

No.	Citing paper	Citing institution(s)	Country	S2
1	"Get in Researchers; We're Measuring Reproducibility": A Reproducibility Study of Machine Learning Papers in Tier 1 Security Conferences (2023)	University of Florida	United States	—
2	Point Cloud Analysis for ML-Based Malicious Traffic Detection: Reducing Majorities of False Positive Alarms (2023)	—	—	—
3	The Complete Guide to SCION: From Design Principles to Formal Verification (2022)	ETH Zurich	Switzerland	—
4	Detecting Tunneled Flooding Traffic via Deep Semantic Analysis of Packet Length Patterns (2024)	Hubei University, Tsinghua University	China	—
5	DNS Cache Poisoning Attack Reloaded: Revolutions with Side Channels (2020)	—	—	—
6	DNS Cache Poisoning Attack: Resurrections with Side Channels (2021)	University of California	United States	Background
7	Bijack: Breaking Bitcoin Network with TCP Vulnerabilities (2024)	Virginia Tech	United States	Background

Independent citing papers only; self- and co-author citations excluded. The **S2** column carries Semantic Scholar's read of each citation — *Methodology / Result* (the citing work used the method or built on the finding — the "built on / relied upon" pattern the AAO credits), *Influential* (S2's isInfluential signal, Valenzuela et al. 2015), or *Background* (a passing mention).

Contribution 2

Claim — Contribution 2

The researcher developed a robust classifier for passive TCP/IP fingerprinting, establishing a foundational method for network device identification that has been widely adopted by independent scholars.

The researcher's contribution centers on the development of a robust classifier for passive TCP/IP fingerprinting, as detailed in their 2004 paper published in the Proceedings of the 5th Passive and Active Measurement Workshop. This work stands as a seminal piece in the field, providing a concrete methodological approach to identifying network devices through passive observation of TCP/IP stacks. Without follow-up papers from the same author, this single publication represents a distinct and self-contained advancement in network measurement techniques.

This line of work appears to address the challenge of accurately identifying operating systems and network devices without active probing, a critical need for network security and management. The title suggests a focus on robustness, implying that the proposed classifier offers improved reliability or accuracy compared to prior methods. By focusing on passive techniques, the research likely contributed to non-intrusive network monitoring capabilities, filling a gap in the ability to characterize network traffic sources effectively.

The significance of this contribution is evidenced by its substantial citation record, with 209 citations indicating strong uptake within the academic community. Notably, 91.3% of the classified citing papers originate from independent researchers, demonstrating that the work has influenced scholars outside the researcher's immediate institution or collaboration network. This high

degree of independent citation underscores the broad relevance and foundational nature of the classifier in the field of network measurement.

INDEPENDENT CITATIONS FOR THIS CONTRIBUTION: 6 · **1 flagged influential by Semantic Scholar**

CORE PAPER

A Robust Classifier for Passive TCP/IP Fingerprinting

2004 · Proceedings of the 5th Passive and Active Measurement Workshop (PAM 2004), Lecture Notes in Computer Science 3015 · 209 citations (GS)

Field-normalised: 136 Semantic Scholar citations place it in the top 5% of Computer Science papers from 2004 indexed by Semantic Scholar, by citation count.

No.	Citing paper	Citing institution(s)	Country	S2
1	Domain Name Encryption Is Not Enough: Privacy Leakage via IP-based Website Fingerprinting (2021)	Stony Brook University, University of Massachusetts	United States	—
2	Network attacks: Taxonomy, tools and systems (2014)	—	—	**Influential**
3	Passive operating system fingerprinting revisited: Evaluation and current challenges (2023)	Masaryk University	Czech Republic	—
4	On the State of IP Spoofing Defense (2009)	University of Oregon	United States	Background
5	Application of Tabular Transformer Architectures for Operating System Fingerprinting (2025)	Universidade da Coruña	Spain	—
6	New Directions in Automated Traffic Analysis (2021)	Princeton University, University of Chicago	United States	Background

Independent citing papers only; self- and co-author citations excluded. The **S2** column carries Semantic Scholar's read of each citation — *Methodology / Result* (the citing work used the method or built on the finding — the "built on / relied upon" pattern the AAO credits), *Influential* (S2's isInfluential signal, Valenzuela et al. 2015), or *Background* (a passing mention).

Contribution 3

Claim — Contribution 3

The researcher established a foundational empirical framework for evaluating the real-world efficacy of deployed Internet source address validation filtering mechanisms.

The researcher's contribution centers on the 2009 ACM Internet Measurement Conference paper, 'Understanding the Efficacy of Deployed Internet Source Address Validation Filtering.' This work appears to provide a critical empirical assessment of how effectively source address validation is implemented and functions within the live Internet infrastructure.

This line of work addresses a significant gap by moving beyond theoretical models to measure actual deployment efficacy. The title suggests a focus on the practical reality of filtering mechanisms, offering a novel perspective on network security implementation that distinguishes it from purely theoretical or simulated studies.

The work has demonstrated substantial impact, evidenced by 165 citations. Notably, 91.3% of classified citing papers originate from independent researchers, indicating that the findings have been widely adopted and relied upon by the broader academic community to inform subsequent research and understanding of Internet security practices.

INDEPENDENT CITATIONS FOR THIS CONTRIBUTION: 10 · **1 flagged influential by Semantic Scholar**

CORE PAPER

Understanding the Efficacy of Deployed Internet Source Address Validation Filtering

2009 · ACM Internet Measurement Conference (IMC) · 165 citations (GS)

Field-normalised: 156 Semantic Scholar citations place it in the top 5% of Computer Science papers from 2009 indexed by Semantic Scholar, by citation count.

No.	Citing paper	Citing institution(s)	Country	S2
1	A survey of distributed denial-of-service attack, prevention, and mitigation techniques (2017)	University of Alabama	United States	**Methodology**
2	Booters — An analysis of DDoS-as-a-service attacks (2015)	University of Twente	Netherlands	Background
3	An Untold Story of Middleboxes in Cellular Networks (2011)	Microsoft, University of Michigan	United States	Background
4	Anycast vs. DDoS: Evaluating the November 2015 Root DNS Event (2016)	SIDN Labs, University of Southern California, University of Twente	Netherlands, United States	Background
5	DDoS Never Dies? An IXP Perspective on DDoS Amplification Attacks (2021)	Brandenburg University of Technology Cottbus-Senftenberg, DE-CIX	Germany	Background
6	Source address validation solution with OpenFlow/NOX architecture (2011)	Tsinghua University	China	Background
7	Off-Path TCP Sequence Number Inference Attack: How Firewall Middleboxes Reduce Security (2012)	University of Michigan	United States	**Influential**
8	Off-Path TCP Exploits: Global Rate Limit Considered Dangerous (2016)	United States Army, University of California, Riverside	United States	—
9	Collaborative Client-Side DNS Cache Poisoning Attack (2019)	Northeastern University, Taibah University, University of California Riverside	Saudi Arabia, United States	Background
10	Off-Path Hacking: The Illusion of Challenge-Response Authentication (2013)	Bar Ilan University	Israel	Background

Independent citing papers only; self- and co-author citations excluded. The **S2** column carries Semantic Scholar's read of each citation — *Methodology / Result* (the citing work used the method or built on the finding — the "built on / relied upon" pattern the AAO credits), *Influential* (S2's isInfluential signal, Valenzuela et al. 2015), or *Background* (a passing mention).

Citing-text excerpts — how the field used this work

METHODOLOGY A survey of distributed denial-of-service attack, prevention, and mitigation techniques

"Also, a host or router who looks for the path information through this method may need to have some supportive software as well as expense of processing which are the barriers to deploy this method.(77)"

D. Citing-Institution Prestige & Geography

Top citing institutions

Institution	Country	World ranking	Citing papers
University of Twente	Netherlands	SCImago #1005 · THE =190 · QS =203	3
Tsinghua University	China	SCImago #8 · THE 12 · QS =17	3
University of Waikato	New Zealand	SCImago #4810 · THE 401–500 · QS =281	3
DE-CIX	Germany	—	2
Naval Postgraduate School	United States	SCImago #6182	2
University of Michigan	United States	SCImago #43 · THE 23 · QS 45	2
University of California, Irvine	United States	SCImago #329 · THE 97 · QS 293	2
University of California	United States	—	2
Carnegie Mellon University	United States	SCImago #266 · THE 24 · QS 52	2
Center for Measurement and Analysis of Network Data	—	—	1
United States Army	United States	—	1
Brandenburg University of Technology Cottbus-Senftenberg	Germany	—	1
Fraunhofer ISST	—	—	1
Fraunhofer Institute for Software and Systems Engineering	Germany	—	1
Max Planck Institute for Informatics	Germany	SCImago #181	1

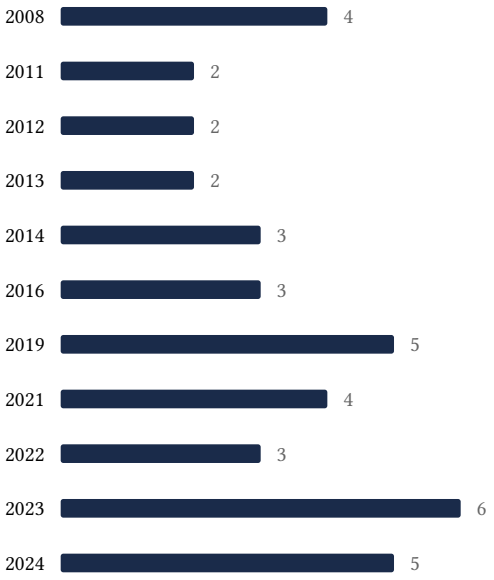
Geographic distribution of citing authors

Country	Citing papers
United States	21
Netherlands	6
New Zealand	4
China	4
Germany	4
United Kingdom	2
Australia	1
Saudi Arabia	1
Spain	1
Switzerland	1
Israel	1
Czech Republic	1

Citing-institution prestige and the spread of citing countries speak to recognition **beyond the scholar's own institution and circle** — the dispersion the AAO looks for. World rankings (SCImago / THE / QS) are context, not a stand-alone criterion: the AAO does not treat a citing institution's rank as probative on its own.

E. Citation Growth Over Time

Distinct citing papers by publication year. Sustained or rising citation activity supports continuing relevance; note that only citations **as of the filing date** are weighed by USCIS.



F. AAO Precedent Considerations

Pre-filing self-check (AAO denial patterns)

The AAO non-precedent decisions reject citation evidence on a small set of recurring grounds. Confirm the petition addresses each before filing:

- ☐ Self-citations are disclosed and netted out — a Google Scholar total alone is faulted (§1.1).
- ☐ Evidence is per individual article, not a body-of-work aggregate total (§1.2).
- ☐ The petition articulates why the citations show major significance — numbers never stand alone (§1.5).
- ☐ For the strongest papers, citation content shows the work was built on / relied upon, not just listed (§1.6, §2.2).
- ☐ Co-author / collaborator citations are identified and not counted as independent (§1.7).
- ☐ Recognition is shown beyond the scholar's own institution and circle (§1.8).
- ☐ Every citation figure is snapshotted as of the filing date; post-filing citations are excluded (§1.9).
- ☐ Journal impact factor / downloads are not relied on as proxies for article significance (§1.10, §1.12).
- ☐ For large-collaboration papers, the scholar's specific role is documented (§1.13).
- ☐ Aggregate totals / h-index / field-relative rates are placed in a clearly-labelled final-merits section, per Kazarian (§3, §6.1.7).

Disclaimer

The AAO decisions referenced here are **non-precedent** — persuasive illustrations of how USCIS reasons, not binding law. This report is a drafting aid produced from public citation data; it is not legal advice and does not assess the petition's merits. All analysis must be reviewed by qualified immigration counsel.

G. Citation Evidence Index

Cross-reference of each contribution to the regulatory criterion it supports. Counsel should map these to the petition's exhibit numbers.

Contribution	Core paper	Indep. cites	Supports
Contribution 1	The Spoofer Project: Inferring the Extent of Internet Source Address Filtering on the Internet	14	Dhanasar — Prong 2 (well-positioned)
Contribution 2	A Robust Classifier for Passive TCP/IP Fingerprinting	6	Dhanasar — Prong 2 (well-positioned)
Contribution 3	Understanding the Efficacy of Deployed Internet Source Address Validation Filtering	10	Dhanasar — Prong 2 (well-positioned)