SecureNT: Smart Topology Obfuscation for Privacy-Aware Network Monitoring

Chengze Du[1], Jibin Shi[2], Hui Xu[3,✉], Guangzhen Yao[4,✉]

[1] School of Cyberspace Security, Beijing University of Posts and Telecommunications, China
ducz0338@bupt.edu.cn
[2] School of Artificial Intelligence, Xidian University, China
zround@stu.xidian.edu.cn
[3] Smart Welfare Collaborative Research Center, Changchun Humanities and Sciences College, China
xuh504@nenu.edu.cn
[4] College of Science, National University of Defense Technology, China
yaoguangzhen@nenu.edu.cn

Abstract. Network tomography plays a crucial role in network monitoring and management, where network topology serves as the fundamental basis for various tomography tasks including traffic matrix estimation and link performance inference. The topology information, however, can be inferred through end-to-end measurements using various inference algorithms, posing significant security risks to network infrastructure. While existing protection methods attempt to secure topology information by modifying end-to-end measurements, they often require complex computation and sophisticated modification strategies, making real-time protection challenging. Moreover, these modifications typically render the measurements unusable for network monitoring, even by trusted users. This paper presents a novel privacy-preserving framework that addresses these limitations. Our approach provides efficient topology protection while maintaining the utility of measurements for authorized network monitoring. Through extensive evaluation on both simulated and real-world networks, we demonstrate that our framework achieves superior privacy protection compared to existing methods while enabling trusted users to effectively monitor network performance. Our solution offers a practical approach for organizations to protect sensitive topology information without sacrificing their network monitoring capabilities. Source code is available at https://gitee.com/Monickar/secure-nt.

Keywords: Privacy-Utility Trade-off, Network Communication, Topology Protect

1 Introduction

Network tomography has emerged as a crucial technique for understanding and monitoring large-scale networks through end-to-end measurements [4]. By ana-

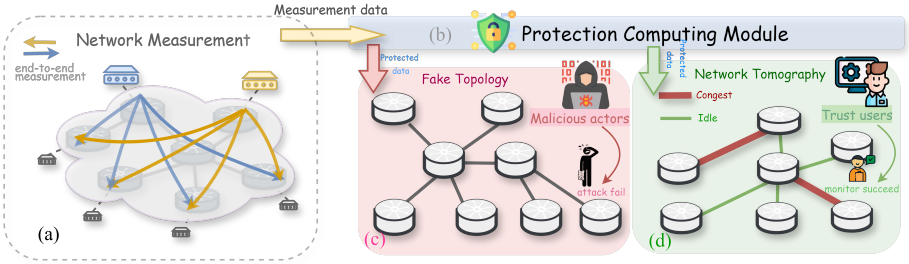

Fig. 1. Overview of our framework: (a) Network Measurement component collecting end-to-end measurements across network paths. (b) Protection Computing Module that processes measurement data. (c) Fake Topology presented to malicious actors, causing their attacks to fail. (d) Network Tomography allowing trusted users to successfully monitor network status, identifying congested and idle links.

lyzing these measurements, network operators can infer internal network characteristics without requiring direct access to network elements. This non-intrusive approach has become increasingly important as networks grow in complexity and scale, particularly in scenarios where direct measurement of network components is impractical or impossible. Central to the effectiveness of network tomography is its reliance on accurate network structural information.

Recent years have seen significant advancement in topology inference methods. Researchers have developed various classic approaches to infer network topology from end-to-end measurements [2, 15, 20]. These inference techniques have become increasingly sophisticated, combining multiple measurement types and leveraging machine learning approaches [1, 11] to improve accuracy.

However, the exposure of topology information presents significant security vulnerabilities that malicious actors could exploit. Malicious actors who can infer network topology potentially identify critical network components [7], discover potential attack vectors [3], or plan targeted disruptions of network services [16]. This vulnerability is particularly concerning as topology information can reveal the hierarchical structure of networks, including critical paths and potential single points of failure [6]. Furthermore, knowledge of network topology can facilitate various attacks, such as traffic analysis, denial of service attacks, or targeted infrastructure compromise [19].

To counter these inference capabilities, several protection approaches have been proposed [5, 10, 17]. Current protection methods typically focus on modifying end-to-end measurements to obscure topology information. However, these approaches face significant limitations. Most notably, they often require complex computation to determine appropriate modifications, making real-time protection challenging. Additionally, these methods ignore the topology protection lies in the inherent trade-off between privacy and utility, which often significantly degrade the quality of network measurements in their attempt to protect topology information. This degradation poses a particular problem for network operators

who need accurate measurements for legitimate monitoring and management tasks. The challenge becomes even more acute when considering environments where both trusted and untrusted users need to work with the same measurement data, but with enough accurate to classify whether the probe is malicuous.

Given these challenges, we propose a privacy-preserving framework and mechanism for network tomography (**SecureNT**, seen in Fig 1). First, the protection mechanism operates in real-time, providing immediate safeguarding of topology information as measurements are taken. This feature is critical for preventing temporal analysis attacks that could exploit delays in implementing protection. Second, our solution maintains measurement utility for trusted users, ensuring that operators and legitimate monitoring systems can accurately assess network performance and identify issues, even while topology information remains inaccessible to unauthorized users. Achieving this balance requires careful trade-offs between data modification and data usability. Third, the protection mechanism effectively prevents topology inference by attackers while remaining resilient to various inference techniques. This includes protection against both current methods and potential future approaches that might leverage advanced analysis techniques or combine different types of measurements. Finally, our solution is computationally efficient, imposing minimal overhead on both processing and network resources. This efficiency is essential for practical deployment in real-world networks, where resources are limited, and performance impacts must be minimized.

Contribution The main contributions of this paper are as follows:

- ***Framework*** We propose a novel privacy-preserving framework for network tomography that effectively protects topology information while maintaining measurement utility.
- ***Mechanism*** We design an efficient mechanism that provides real-time protection without requiring complex computation or sophisticated modification strategies.
- ***Evaluation*** Through extensive evaluations, we demonstrate that our framework achieves superior protection while maintaining measurement utility for trusted users.

2 Related Work

Network topology inference and obfuscation represent two interrelated areas of network research.

Topology Inference Network topology inference has been extensively studied in network tomography, with early methods relying on additive metrics to formulate the problem as a linear inverse task, leveraging the known link-path relationships. Techniques such as Maximum Likelihood Estimation (MLE) [2] and Expectation Maximization (EM) [20] were employed for robust topology reconstruction, while algebraic methods like Systems of Linear Equations (SLE) effectively addressed scenarios with sparse measurements [15]. Machine learning-based methods have further advanced the field by overcoming limitations of

traditional approaches. For example, NeuTomography [12] and DeepNT [1] employ deep neural architectures to infer network structures and predict path performance without prior topology knowledge, offering enhanced scalability and adaptability to diverse network conditions. These advancements demonstrate the evolution from statistical and algebraic methods to more flexible, data-driven approaches for network topology inference.

Topology Obfuscation Recent advancements in network topology obfuscation have emerged to counter various adversarial inference attacks using diverse strategies. Techniques such as AntiTomo [10] and Proto [5] strategically manipulate end-to-end delay measurements to mislead attackers while preserving the real topology, whereas EigenObfu [23] explicitly modifies graph structures to generate convincing fake topologies. While these methods primarily address static network representations, HBB-TSP [9] addresses the high-order adaptability limitation by leveraging dynamic hypergraphs for real-time obfuscation of critical links. Complementary approaches such as NetHide [13] and CHAOS [18] provide optimization-driven and SDN-based moving target defenses, respectively, while methods like PINOT [21] and Attack Graph Obfuscation [17] focus on achieving an optimal balance between anonymity, routing efficiency, and deceptive resource allocation.

3 Preliminaries and Problem Definition

3.1 Network Model and Performance Inference

We consider a network represented as an undirected graph $\mathcal{G} = (\mathcal{N}, \mathcal{L})$, where $\mathcal{N}$ represents the set of nodes (such as routers, switches, and hosts) and $\mathcal{L}$ denotes the set of links connecting these nodes. Within this network, source nodes generate data flows that traverse through the network to reach destination nodes. Each direct connection between two nodes is represented by a link $l \in \mathcal{L}$.

A path p is defined as an ordered set of links that connect a source-destination pair, and we denote the set of all paths in the network as $\mathcal{P}$. The relationship between paths and links is captured by the routing matrix $\mathbf{R} \in \{0,1\}^{|\mathcal{P}|\times|\mathcal{L}|}$. If the element in the i-th row and j-th column of $\mathbf{R}$ is 1, it indicates that the i-th path contains the j-th link; otherwise, it is 0.

In network tomography, the goal is to infer link-level performance metrics $\mathbf{X} \in \mathbb{R}^{|\mathcal{L}|}$ from end-to-end path measurements $\mathbf{Y} \in \mathbb{R}^{|\mathcal{P}|}$. This relationship can be expressed as:

$$y_i = \bigodot_{j=1}^{|\mathcal{L}|} R_{ij} \cdot x_j \Longrightarrow \mathbf{Y} = \mathbf{R} \bigodot \mathbf{X} \tag{1}$$

where $\bigodot$ represents an operation that varies depending on the performance metric being considered. For additive metrics such as delay, $\bigodot$ represents summation, whereas for metrics like capacity, it could represent a minimum operation. Each element y_i represents the end-to-end measurement on path i, and each element x_j represents the performance metric (such as delay or capacity)

on link j. This inference process critically depends on knowledge of the routing matrix $\mathbf{R}$, which is derived directly from the network topology. This fundamental relationship between topology and performance inference underlies both the utility of network tomography for legitimate monitoring and its vulnerability to topology inference attacks.

3.2 Attacker Model and Topology Inference

In our threat model, the attacker aims to infer the network topology $\mathcal{G}$ by analyzing end-to-end measurements $\mathbf{Y}$. Although the attacker lacks direct knowledge of the routing matrix $\mathbf{R}$ or the topology $\mathcal{G}$, they employ an inference algorithm $f(\cdot)$ to estimate the routing matrix $\hat{\mathbf{R}}$ and reconstruct the topology $\hat{\mathcal{G}}$. This inference process can be expressed as:

$$\hat{\mathcal{G}} = f(\mathbf{Y}), \quad \text{where } \hat{\mathcal{G}} = \left\{\hat{\mathcal{N}}, \hat{\mathcal{L}}, \hat{\mathbf{R}}\right\}, \tag{2}$$

with $\hat{\mathcal{N}}$, $\hat{\mathcal{L}}$, and $\hat{\mathbf{R}}$ representing the inferred nodes, links, and routing matrix, respectively. The inference process leverages temporal correlations in measurements, statistical properties of end-to-end delays, and patterns in performance metrics across different paths to improve the accuracy of the reconstruction.

The effectiveness of the attack is measured by comparing the inferred topology $\hat{\mathcal{G}}$ with the actual topology $\mathcal{G}$. This comparison uses a similarity measure defined as:

$$\text{Similarity}(\mathcal{G}, \hat{\mathcal{G}}) = s(\mathcal{G}, \hat{\mathcal{G}}) = 1 - \frac{G_0}{G_1 + G_2}, \tag{3}$$

where $s(\mathcal{G}, \hat{\mathcal{G}})$ is based on a graph edit distance-inspired metric.G_0 quantifies the cost of transforming the actual topology $\mathcal{G}$ into the inferred topology $\hat{\mathcal{G}}$, G_1 represents the cost of removing all nodes and links from $\mathcal{G}$ to obtain an empty graph, and G_2 denotes the cost of constructing $\hat{\mathcal{G}}$ from an empty graph. The similarity score ranges from 0 to 1. A value of 1 indicates that the inferred topology $\hat{\mathcal{G}}$ is identical to the actual topology $\mathcal{G}$, whereas smaller values signify greater structural differences between the two graphs. This similarity measure offers a flexible and intuitive way to assess the success of topology inference attacks, where a high similarity score reflects the attacker's ability to accurately reconstruct the network, underscoring the importance of robust protection mechanisms.

4 METHODOLOGY

4.1 Path Relationship-based Noise Injection

To protect the real topology from inference attacks, we introduce a fake topology represented by another routing matrix $\mathbf{R}' \in \mathbb{R}^{|P| \times |L'|}$, where L' denotes the fake links. A plausible fake link-delay vector $\mathbf{X}' \in \mathbb{R}^{|L'|}$ is generated based on

properties like link lengths, and the fake path measurements $\mathbf{Y}' \in \mathbb{R}^{|P|}$ are computed as follows:

$$x'_j = \frac{c}{l'_j + 1} \Rightarrow y'_i = \bigodot_{j=1}^{|\mathcal{L}'|} \mathbf{R}'_{ij} \cdot x'_j \Rightarrow \delta_y = \mathbf{R}' \bigodot \mathbf{X}' \tag{4}$$

where $L'_j > 0$ is the length of the j-th fake link, and c is a scaling constant. This process assigns smaller delays to longer links and larger delays to shorter links, mimicking realistic variability in network delays.

To ensure that the noise δ_y blends smoothly with the true path measurements $\mathbf{Y}$ and reduces statistical differences, it is scaled and smoothed using a mechanism M. The final modified measurements are expressed as:

$$\tilde{\mathbf{Y}} = \mathbf{Y} + \delta_y^{\text{adj}} = \mathbf{R} \bigodot \mathbf{X} + \alpha M \delta_y \tag{5}$$

where α adjusts the noise magnitude, and M serves as a proctection computing moduel, which two distributions A and B as inputs and iteratively applies gradient descent with a projection step to minimize the L2 loss between them. This is achieved using two input distributions: the fake measurements $\mathbf{R}'\mathbf{X}'$ and the reference measurements $\mathbf{RI}$, where $\mathbf{I} \in \mathbb{R}^{|L'|}$ is a vector of ones. The adjusted noise δ_y^{adj} is computed as:

$$\delta_y^{\text{adj}} = M(\mathbf{R}' \bigodot \mathbf{X}', \mathbf{R} \bigodot \mathbf{I}) \tag{6}$$

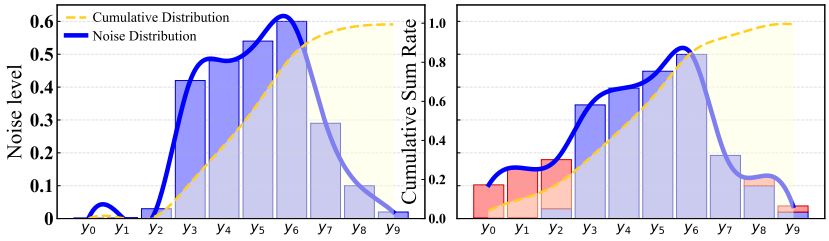

Fig. 2. Noise between AntiTomo (left) and SecureNT (right). SecureNT implements path length-aware noise smoothing to achieve balanced noise distribution while preserving overall noise scale. Blue solid lines show the probability density of noise distribution, and yellow dashed lines represent cumulative distribution functions. The red shaded regions in the right subplot highlight the additional noise compensation introduced by SecureNT compared to AntiTomo.

4.2 Protection Objectives

The noise injection mechanism is designed to achieve three intertwined objectives, which can be expressed as:

$$\mathbf{Y}_{best} = \min_{\mathbf{Y}'} \|\mathbf{Y}' - \mathbf{Y}\| - \lambda_1 d(\mathcal{G}, \mathcal{G}') + \lambda_2 \|\hat{\mathbf{X}}_t - \mathbf{X}\| \tag{7}$$

Algorithm 1: Protection Computing Moduel

Input : Initial distribution $\mathbf{Y}$, target distribution $\mathbf{RI}$, convergence threshold γ

Output: Adjusted distribution $\mathbf{Y}'$

/* Initialize and Compute Initial Loss */

Set the initial total of $\mathbf{Y}$, $\mathbf{RI}$ to $\mathbb{S}(\mathbf{Y})$ $\mathbb{S}(\mathbf{RI})$;

Set $\alpha \leftarrow \frac{\mathbb{S}(\mathbf{RI})}{\mathbb{S}(\mathbf{Y})} \longrightarrow \mathbf{Y} \leftarrow \mathbf{Y} \times \alpha$; /* Scale Y to match sum of RI */

Set the initial loss $\mathcal{L}_{\text{initial}} \leftarrow \mathcal{L}(\mathbf{Y}, \mathbf{RI})$;

/* Iterative Gradient Descent with Projection */

for $t = 1$ ***to*** T_{max} **do**

  Compute the gradient: $\nabla\mathcal{L}(\mathbf{Y}, \mathbf{RI}) = 2(\mathbf{Y} - \mathbf{RI})$;

  Update $\mathbf{Y}$: $\mathbf{Y} \leftarrow \mathbf{Y} - \eta \cdot \nabla\mathcal{L}(\mathbf{Y}, \mathbf{RI})$

  /* Projection to maintain the sum of Y */

  Compute the current total: $\mathbb{S}(\mathbf{Y}') \leftarrow \mathbb{S}(\mathbf{Y})$;

  Adjust $\mathbf{Y} : \mathbf{Y} \leftarrow \mathbf{Y} \times \frac{\mathbb{S}(\mathbf{RI})}{\mathbb{S}(\mathbf{Y}')}$;

  /* Convergence Check */

  Compute the current loss: $\mathcal{L}_{\text{current}} \leftarrow \mathcal{L}(\mathbf{Y}, \mathbf{RI})$;

  if $\mathcal{L}_{current} \leq \gamma \cdot \mathcal{L}_{initial}$ **then**

    break ; /* Converged, exit loop */

return Y

where λ_1 and λ_2 are weighting factors that balance the importance of topology protection ($d(\mathcal{G}, \mathcal{G}')$) and performance inference accuracy ($\|\hat{\mathbf{X}}_t - \mathbf{X}\|$) against the need to preserve measurement fidelity ($\|\mathbf{Y}' - \mathbf{Y}\|$). First, measurement fidelity is preserved by minimizing the difference between the modified and original measurements, ensuring $\|\mathbf{Y}' - \mathbf{Y}\|$ remains small. Second, topology protection is maximized by increasing the difference between the real topology $\mathcal{G}$ and the topology $\mathcal{G}'$ inferred from the modified measurements, represented as $\max d(\mathcal{G}, \mathcal{G}')$, where $d(\cdot, \cdot)$ is a topology distance metric. Third, performance inference accuracy for trusted users is maintained by minimizing the error between the true link performance $\mathbf{X}$ and the inferred link performance $\hat{\mathbf{X}}_t$, ensuring $\|\hat{\mathbf{X}}_t - \mathbf{X}\|$ remains small. These objectives are carefully balanced through the design of the noise function $\eta_i(r_i)$, which scales with relationship strength to maximize topology protection while maintaining bounded noise to preserve fidelity and the utility of the measurements for trusted users.

5 Evaluation

5.1 Datasets and Comparative Methods

Our evaluation uses real-world network topologies from the Internet dataset Topology Zoo [8], which provides a diverse set of network configurations. We se-

lect 4 representative topologies, to ensure a thorough assessment of the proposed method. These topologies are summarized in Table 1, covering various scales and structural complexities.

Table 1. Characteristics of four real networks used for numerical simulations.

Mec. \ Net.	CHINANET	AGIS	GANET	ERNET
#Paths	17	14	15	12
#Links	21	18	17	13
Avg.Hops	3.9	3.6	3.6	3.25
Avg.Weights	4.3	2.8	3.1	3

We compare our approach with two state-of-the-art topology inference methods and two existing protection methods. For inference, we use **Maximum Penalized Likelihood (MPL)** as inference algorithm, which was a classical statistical approach that infers topology by maximizing the likelihood of observed end-to-end measurements. For protection, we include **AntiTomo**, which employs multi-objective optimization to manipulate delay measurements for topology protection, and **Proto**, a strategy-based method that introduces delays to create misleading topological impressions.

All methods were implemented in Python, with path measurements generated using NS-3, and experiments conducted on Linux.

5.2 Topology Protection Effectiveness

We futher evaluate topology protection effectiveness using Similarity Scores, which measure the similarity between the inferred and true network topologies. A lower similarity score indicates more effective protection, as it means the attacker's inferred topology differs more from the actual network structure.

Figure 3 demonstrates the comparative performance of different protection methods across four network topologies (GANET, AGIS, CHAINET, and ERNET). The baseline case without protection (dashed black line) shows that attackers can achieve nearly perfect topology inference (similarity scores approaching 1.0) as the number of probe packets increases. Our proposed SecureNT method (red line) consistently outperforms Proto (blue line) and achieves performance comparable to AntiTomo (green line) across all evaluated networks.

For smaller networks like AGIS and GANET, SecureNT achieves an average topology similarity of 78.2%, which is comparable to AntiTomo (77.8%) and notably better than Proto (82.5%). The protection effectiveness remains robust for larger networks like CHAINET and ERNET, where SecureNT maintains a similarity score of 77.7%, matching AntiTomo's 77.4% while outperforming Proto by 7.2%. On average across all four topologies, SecureNT improves topology protection by 6.7% compared to Proto, achieving an overall similarity score of 78.7%.

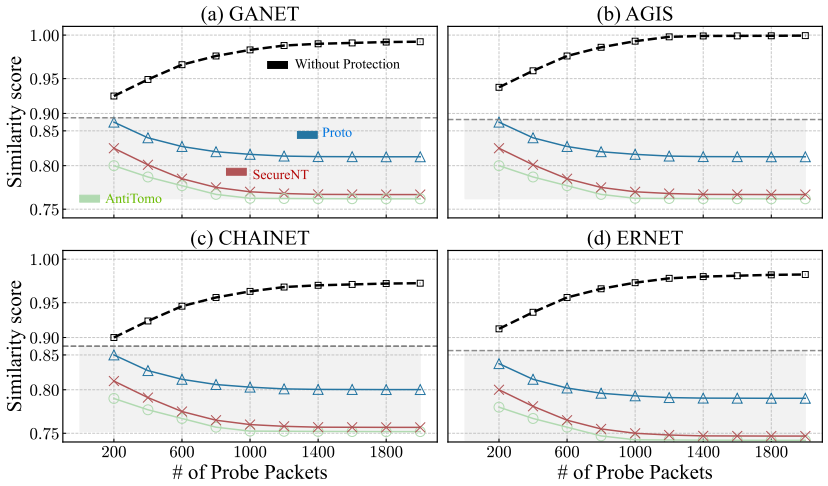

Fig. 3. Comparison of topology protection effectiveness on four network topologies under varying numbers of probe packets. Lower similarity scores indicate better protection performance.

Importantly, the graphs show that SecureNT's performance remains stable even as the number of probe packets increases from 200 to 1800, demonstrating consistent protection regardless of the intensity of probing attempts. This stability across different network sizes and probing intensities confirms that SecureNT provides reliable defense against topology inference attacks.

5.3 Measurement Utility for Trusted Users

To comprehensively evaluate how well our protection mechanism preserves measurement utility for trusted users, we analyze both binary congestion detection accuracy and continuous link performance inference capability.

For binary congestion detection, we employ the CLINK [14] algorithm, which determines link congestion status based on end-to-end measurements and network topology. Figure 4 presents the F1-scores across four network topologies under both low and high congestion conditions. The baseline case (Without Protection) achieves F1-scores of approximately 0.87 in low congestion scenarios but drops to 0.75-0.77 under high congestion, reflecting the inherent challenges of congestion detection under heavy network load.

SecureNT demonstrates superior utility preservation compared to existing approaches. Under low congestion conditions, it maintains F1-scores of 0.83-0.85 for smaller networks (GANET and AGIS) and 0.80-0.82 for larger networks (CHAINET and ERNET), representing only a 7-10% decrease from the baseline. In contrast, AntiTomo and Proto show larger performance degradation of 12-15%. The advantage becomes more pronounced under high congestion scenar-

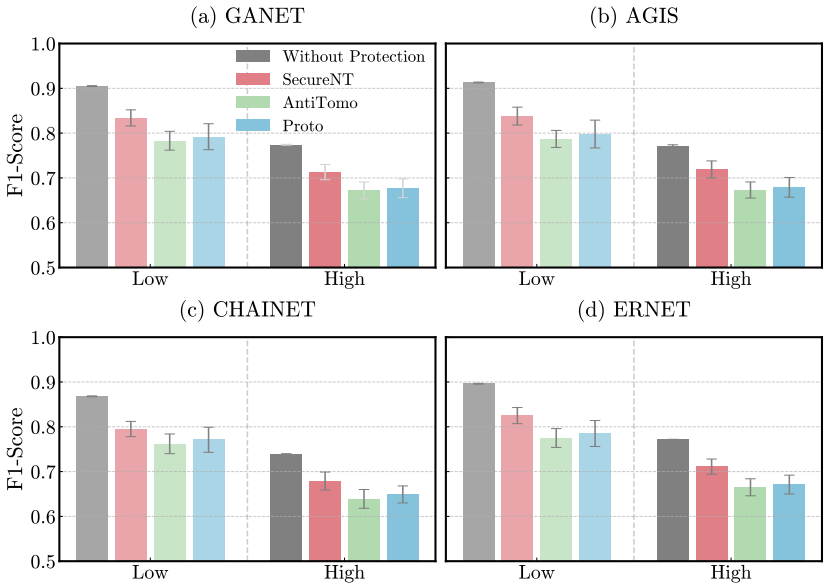

Fig. 4. F1-scores of link congestion detection under low and high congestion levels across four network topologies, comparing Normal Tomography with three protection methods.

ios, where SecureNT maintains F1-scores around 0.70-0.72 across all topologies, consistently outperforming other methods.

For continuous link performance inference, we quantify accuracy using the normalized root mean square error (NRMSE):

$$\text{NRMSE} = \sqrt{\frac{\sum_{m=0}^{M-1} |y[m] - \hat{y}[m]|^2}{\sum_{m=0}^{M-1} |y[m]|^2}}$$

where $y[m]$ represents the true link performance and $\hat{y}[m]$ represents the inferred performance. Figure 5 shows how different protection methods affect RangeTomo [22] 's inference accuracy under varying link congestion probabilities. For moderate congestion probabilities (0.1-0.3), SecureNT maintains inference accuracy above 70% across all networks, while AntiTomo and Proto drop below 65%. At higher congestion probabilities (0.5), SecureNT preserves inference similarity around 55-60% while other methods deteriorate to 45-50%.

5.4 Computational Efficiency

We evaluate computational efficiency of protection methods by measuring execution times across network topologies under low/high congestion. As shown in Table 2, SecureNT ($\gamma = 0.6$) outperforms baselines consistently, requiring only 98.40 s versus 140.32 s/115.47 s (AntiTomo/Proto) for CHINANET

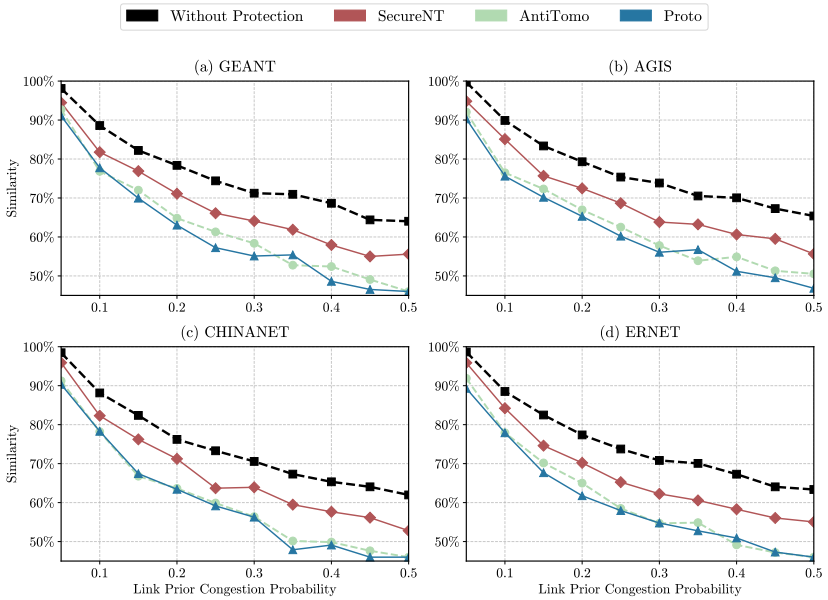

Fig. 5. Impact of protection methods on link performance inference accuracy across four network topologies.

under low congestion. The advantage expands under high congestion (105.34 s versus 184.75 s/143.45 s).

The parameter γ balances speed and protection quality: $\gamma = 0.4$ yields slightly longer times (108.40 s versus 98.40 s for CHINANET low congestion) while remaining faster than baselines. Increasing to $\gamma = 0.6$ reduces processing time by 8–10% across topologies with minimal utility trade-off.

SecureNT's efficiency stems from direct noise injection, avoiding complex optimization. This enables real-time protection updates even in large dynamic networks like CHINANET, maintaining practical execution times ($\leq$105 s) under high congestion—critical for real-world deployment.

6 Conclusion

In this paper, we proposed a privacy-preserving framework for network tomography that achieves real-time topology protection while maintaining the utility of measurements for trusted users. Our approach effectively defends against both current and emerging topology inference techniques, ensuring robust privacy without compromising network monitoring capabilities. Extensive evaluations on simulated and real-world networks topology demonstrated the framework's superior privacy protection, usability, and computational efficiency, making it practical for deployment in real-world scenarios. This work addresses critical

Table 2. Execution time (seconds) comparison of protection methods across different network topologies.

Topo. \ Alg.	Low Congestion				High Congestion			
	AntiTomo	Proto	SecureNT		AntiTomo	Proto	SecureNT	
			$\gamma = 0.4$	$\gamma = 0.6$			$\gamma = 0.4$	$\gamma = 0.6$
CHINANET	140.32	115.47	108.40	**98.40**	184.75	143.45	124.12	**105.34**
GANET	130.21	102.67	95.56	**86.92**	165.43	128.90	110.34	**92.45**
ERNET	135.43	108.78	98.34	**90.62**	170.78	135.34	115.67	**97.23**
AGIS	125.89	95.54	90.67	**82.32**	158.54	120.32	105.45	**88.76**

challenges in network security and monitoring, providing a foundation for future advancements in balancing privacy and performance in large-scale networks.

References

1. Anonymous. DeepNT: Path-centric graph neural networks for network tomography. In *Submitted to The Thirteenth International Conference on Learning Representations*, 2024. under review.
2. Mark Coates, Rui Castro, Robert Nowak, Manik Gadhiok, Ryan King, and Yolanda Tsang. Maximum likelihood network topology identification from edge-based unicast measurements. *ACM SIGMETRICS Performance Evaluation Review*, 30(1):11–20, 2002.
3. Shuhua Deng, Wenjie Dai, Xian Qing, and Xieping Gao. Vulnerabilities in sdn topology discovery mechanism: Novel attacks and countermeasures. *IEEE Transactions on Dependable and Secure Computing*, 2023.
4. Ting He, Liang Ma, Ananthram Swami, and Don Towsley. *Network tomography: identifiability, measurement design, and network state inference*. Cambridge University Press, 2021.
5. Tao Hou, Zhe Qu, Tao Wang, Zhuo Lu, and Yao Liu. Proto: Proactive topology obfuscation against adversarial network topology inference. In *IEEE INFOCOM 2020-IEEE Conference on Computer Communications*, pages 1598–1607. IEEE, 2020.
6. Sushil Jajodia and Steven Noel. Topological vulnerability analysis: A powerful new approach for network attack prevention, detection, and response. In *Algorithms, architectures and information systems security*, pages 285–305. World Scientific, 2009.
7. Sushil Jajodia, Steven Noel, and Brian O'berry. Topological analysis of network attack vulnerability. *Managing Cyber Threats: Issues, Approaches, and Challenges*, pages 247–266, 2005.
8. Simon Knight, Hung X. Nguyen, Nickolas Falkner, Rhys Bowden, and Matthew Roughan. The internet topology zoo. *IEEE Journal on Selected Areas in Communications*, page 1765–1775, Oct 2011.
9. Xiaohui Li, Xiang Yang, Yizhao Huang, and Yue Chen. Combating temporal network inference by high-order camouflaged network topology obfuscation. *Available at SSRN 4758548*, 2022.

10. Yaqun Liu, Changyou Xing, Guomin Zhang, Lihua Song, and Hongxiu Lin. Antitomo: Network topology obfuscation against adversarial tomography-based topology inference. *Computers & Security*, 113:102570, 2022.
11. Liang Ma, Ziyao Zhang, and Mudhakar Srivatsa. Neural network tomography. *arXiv preprint arXiv:2001.02942*, 2020.
12. Liang Ma, Ziyao Zhang, and Mudhakar Srivatsa. Neural network tomography. *arXiv preprint arXiv:2001.02942*, 2020.
13. Roland Meier, Petar Tsankov, Vincent Lenders, Laurent Vanbever, and Martin Vechev. {NetHide}: Secure and practical network topology obfuscation. In *27th USENIX Security Symposium (USENIX Security 18)*, pages 693–709, 2018.
14. H. X. Nguyen and P. Thiran. The boolean solution to the congested ip link location problem: Theory and practice. In *IEEE INFOCOM 2007 - 26th IEEE International Conference on Computer Communications*, Jan 2007.
15. Jian Ni, Haiyong Xie, Sekhar Tatikonda, and Yang Richard Yang. Efficient and dynamic routing topology inference from end-to-end measurements. *IEEE/ACM transactions on networking*, 18(1):123–135, 2009.
16. Mahendra Piraveenan, Gnana Thedchanamoorthy, Shahadat Uddin, and Kon Shing Kenneth Chung. Quantifying topological robustness of networks under sustained targeted attacks. *Social Network Analysis and Mining*, 3:939–952, 2013.
17. Rami Puzis, Hadar Polad, and Bracha Shapira. Attack graph obfuscation. *arXiv preprint arXiv:1903.02601*, 2019.
18. Yuan Shi, Huanguo Zhang, Juan Wang, Feng Xiao, Jianwei Huang, Daochen Zha, Hongxin Hu, Fei Yan, and Bo Zhao. Chaos: an sdn-based moving target defense system. *Security and Communication Networks*, 2017(1):3659167, 2017.
19. Swati, Sangita Roy, Jawar Singh, and Jimson Mathew. Design and analysis of ddos mitigating network architecture. *International Journal of Information Security*, 22(2):333–345, 2023.
20. Yolanda Tsang, Mark Coates, and Robert Nowak. Passive network tomography using em algorithms. In *2001 IEEE International Conference on Acoustics, Speech, and Signal Processing. Proceedings (Cat. No. 01CH37221)*, volume 3, pages 1469–1472. IEEE, 2001.
21. Liang Wang, Hyojoon Kim, Prateek Mittal, and Jennifer Rexford. Programmable in-network obfuscation of traffic. *arXiv preprint arXiv:2006.00097*, 2020.
22. Sajjad Zarifzadeh, Madhwaraj Gowdagere, and Constantine Dovrolis. Range tomography: combining the practicality of boolean tomography with the resolution of analog tomography. In *Proceedings of the 2012 Internet Measurement Conference*, pages 385–398, 2012.
23. Ziliang Zhu, Guopu Zhu, Yu Zhang, Jiantao Shi, Xiaoxia Huang, and Yuguang Fang. Eigenobfu: A novel network topology obfuscation defense method. *IEEE Transactions on Network Science and Engineering*, 2024.