**Title:**  
**An Analysis of Packet Count Distribution by Size Across Multiple Network Protocols**

**Abstract:**  
This research presents an in-depth analysis of packet count distribution by size across various network protocols, including HTTP, HTTPS, ICMP, TCP, and UDP. By visualizing the data through a logarithmic scale graph, the study uncovers significant differences in how these protocols manage packet sizes, revealing patterns and tendencies that are crucial for network analysis, traffic characterization, and optimization.

**Introduction**

Network traffic analysis is essential for understanding the behavior of different protocols and optimizing performance. This research focuses on examining the distribution of packet sizes across multiple network protocols, using a log-log scale to highlight patterns and concentrations in packet counts. The protocols under consideration—HTTP, HTTPS, ICMP, TCP, and UDP—are widely used in various applications, making their analysis critical for network management and troubleshooting.

**Methodology**

The analysis was conducted by plotting the packet count distribution against packet size on a logarithmic scale. This approach was chosen to effectively capture the wide range of values typically observed in network traffic, where packet sizes and counts can vary significantly. Each protocol was represented by a distinct color in the graph, enabling clear differentiation and comparison.

**Results and Interpretation**

**Packet Size Distribution**  
The results show that packet sizes span a broad range, with a notable clustering between the log10 scale of approximately 1.5 and 3.2. This indicates that most packets fall within this size range, with a concentration of larger packet sizes (log10 close to 3) across multiple protocols. The dense clustering suggests that larger packets are common, likely due to data-heavy transfers.

**Protocol Distribution**  
The distribution of packet sizes varies significantly across different protocols:

* **HTTP and HTTPS:** These protocols exhibit a broad range of packet sizes, with activity observed across the entire spectrum. This suggests that they handle a diverse set of operations, from small control packets to larger data transfers.
* **ICMP:** This protocol shows activity mainly in the lower to mid-range packet sizes (log10 around 2). ICMP is typically used for diagnostic and control purposes, which may explain its narrower size range.
* **TCP and UDP:** Both protocols span the entire packet size range but are less uniformly distributed compared to HTTP/HTTPS. TCP, known for its reliability, and UDP, known for its simplicity, are used for a variety of applications, leading to diverse packet sizes.

**Log-Scaled Axes**  
The use of logarithmic scales on both axes was crucial for visualizing the data's broad range. This transformation allowed for the compression of data points, making patterns in the distribution more apparent and highlighting the concentration of traffic in certain packet size ranges.

**Patterns**  
The graph reveals that most network traffic is concentrated in higher packet sizes, with multiple protocols overlapping in this range. The spikes observed in the plot likely correspond to common network operations or specific data transfer patterns, where certain packet sizes are more frequent.

**Interpretation**

The findings underscore the diversity in how different protocols handle packet sizes. For example, HTTP/HTTPS protocols manage a wide variety of packet sizes, reflecting their role in web browsing and data transfer. In contrast, ICMP's limited size range is consistent with its use for control messages. The varying distributions observed in TCP and UDP highlight the different applications and use cases these protocols support.

The use of a log-log scale was effective in uncovering these patterns, but further analysis could involve breaking down the data by specific protocols or examining raw packet sizes without the log transformation. This would help identify outliers or more granular patterns that might be obscured in the aggregated data.

**Conclusion**

This research provides valuable insights into the packet size distribution across multiple network protocols, revealing patterns that are crucial for network analysis and optimization. Understanding these variations is essential for developing accurate models and simulations of network traffic, which can be applied to performance optimization, network management, and troubleshooting. Future work could expand on this analysis by exploring additional protocols or examining packet size distributions in different network environments.

**6. References**

* [1] Dainotti, A., Pescapè, A., & Ventre, G. (2006). A packet-level characterization of network traffic. *IEEE CAMAD 2006*, DOI: 10.1109/CAMAD.2006.1649716.
* [2] Paxson, V., & Floyd, S. (1995). Wide area traffic: The failure of Poisson modeling. *IEEE/ACM Transactions on Networking*, 3(3), 226-244.
* [3] Crovella, M., & Bestavros, A. (1997). Self-similarity in World Wide Web traffic: Evidence and possible causes. *IEEE/ACM Transactions on Networking*, 5(6), 835-846.