



Calhoun: The NPS Institutional Archive
DSpace Repository

Faculty and Researchers

Faculty and Researchers' Publications

2016

Identification of Low-Latency Obfuscated Traffic Using Multi-Attribute Analysis

Doherty, Kevin

Monterey, California. Naval Postgraduate School

<http://hdl.handle.net/10945/56292>

This publication is a work of the U.S. Government as defined in Title 17, United States Code, Section 101. Copyright protection is not available for this work in the United States.

Downloaded from NPS Archive: Calhoun



Calhoun is the Naval Postgraduate School's public access digital repository for research materials and institutional publications created by the NPS community. Calhoun is named for Professor of Mathematics Guy K. Calhoun, NPS's first appointed -- and published -- scholarly author.

Dudley Knox Library / Naval Postgraduate School
411 Dyer Road / 1 University Circle
Monterey, California USA 93943

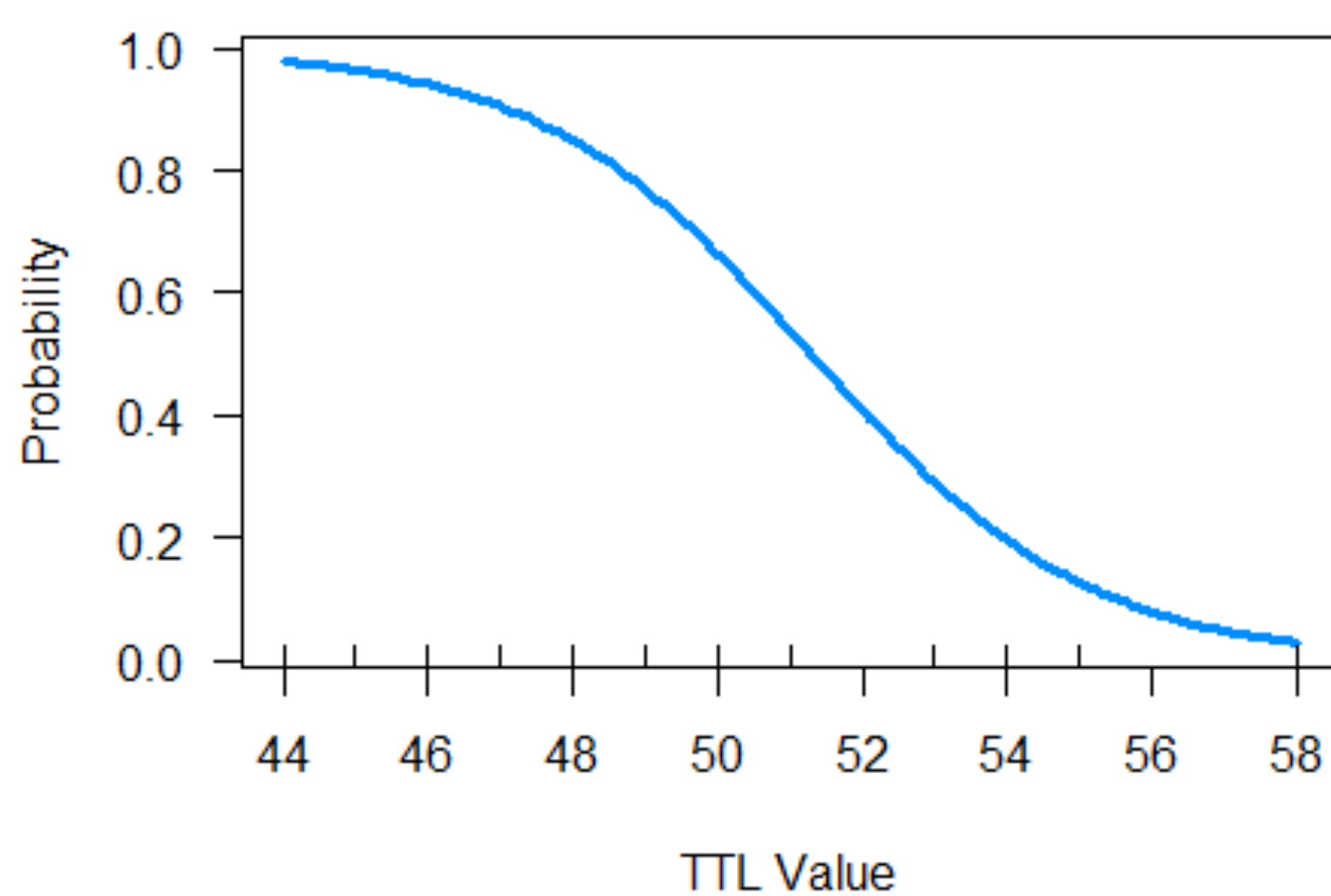
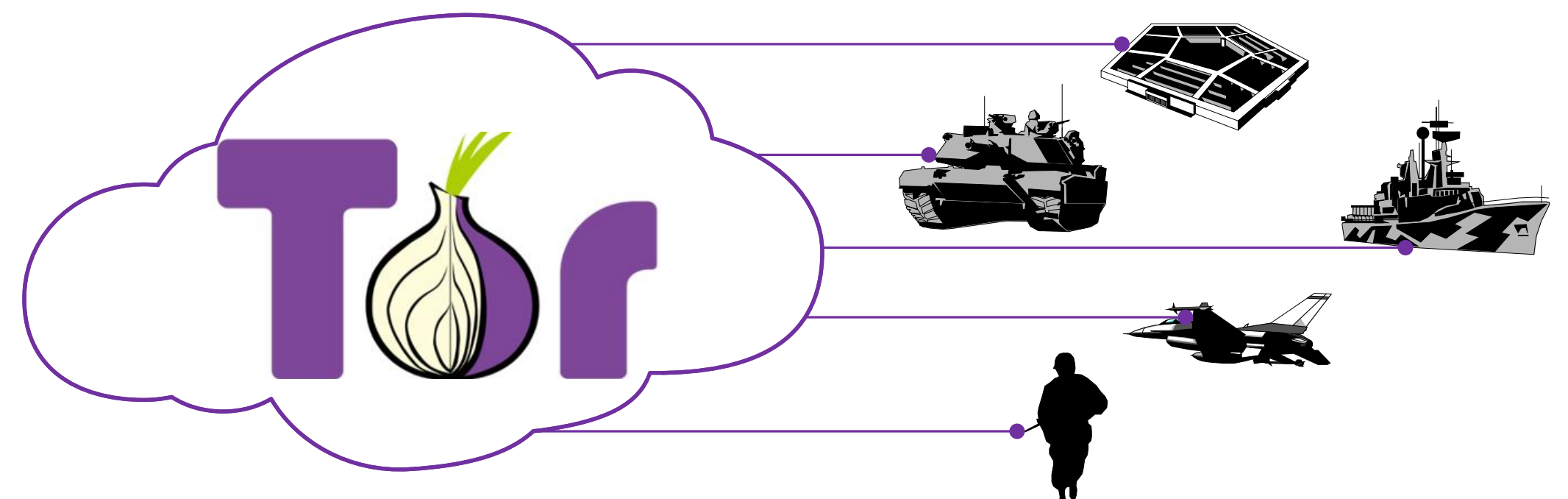
<http://www.nps.edu/library>

Identification of Low-Latency Obfuscated Traffic Using Multi-Attribute Analysis



Real World Threat

- No process or system capable of detecting Tor network traffic on DOD networks.
- The level of unauthorized Tor traffic on DOD networks is unknown. This creates significant risk from both insider-threat and network-defense perspectives.
- Only 14.6 percent of all Tor source IP addresses observed were published on the hourly Tor exit node list — blacklisting is NOT an effective solution.



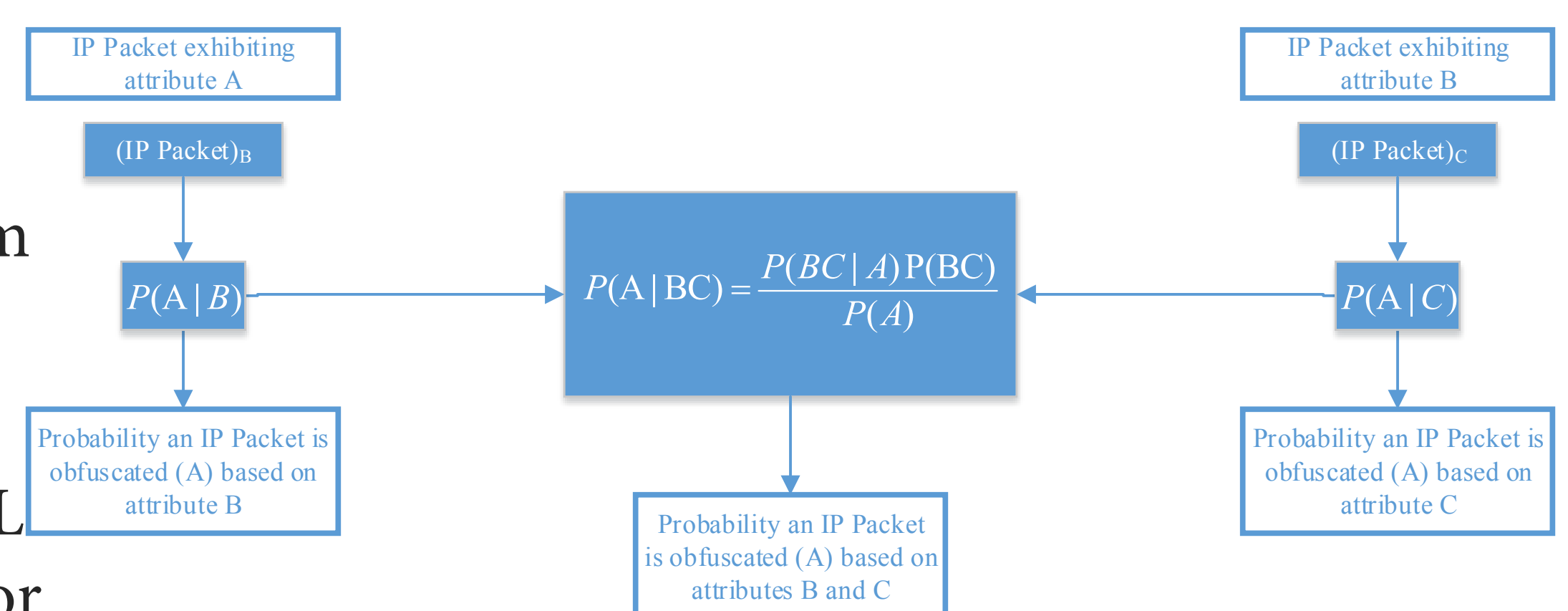
Probability of classification for Tor traffic based on IP TTL

Single Attribute Analysis

- 351,188 unique Tor packets exhibited common characteristics in their IP time-to-live (TTL), TCP offset, and IP packet length fields.
- Each trait was tested to determine its ability to detect Tor traffic in a mixed dataset; this resulted in a 53 to 62.1 percent probability of correctly classifying Tor traffic.
- IP TTL was the best single discriminator to detect Tor traffic which is likely due to the preponderance of Tor exit nodes running Linux; as of January 2017, Linux-based operating systems accounted for 91.3 percent of all Tor exit nodes.

Multi-Attribute Prediction

- Using three pre-filter variations, the observed FPR for non-Tor ranged from 94.4 percent to 7.2 percent, and the observed FNR for Tor ranged from 61.3 percent to 1.6 percent. Interestingly, the tests that used more pre-filters performed the worst.
- Filtering the data set based on common Tor IP TTL values only resulted in a TPR of 91.3 percent for Tor traffic and a FPR of 7.2 percent for non-Tor traffic.



Multi-attribute decision model using Naïve Bayes analysis

- Naïve Bayes multi-attribute prediction model allows maximum flexibility when applying to real-world networks and applications.

Key Takeaways

- Real-time detection of Tor traffic is possible using network traffic analysis.
- Tor traffic has identifiable TPC/IP packet and routing characteristics — more are likely to exist.
- Probability of detection can be increased by evaluating groups of packets from a single source IP all at once — this will examine the behavior from an IP address vice that of each TCP/IP packet.



LT Kevin Dougherty
Graduate School of Operational and Information Sciences

NRP Topic IREF ID: NPS-N16-N201-C
Topic Sponsor: N2/N6- Information Warfare

Faculty Advisors:
Dr. Shelley Gallup, GSOIS
Dr. Tom Anderson, USACE ERDC CRREL
at TRAC MTRY