A NEW METHOD FOR DETECTING AND TRACKING COVERT TERRORIST NETWORKS

Non-proprietary White Paper

Steve Kramer, Ph.D.
Paragon Science, Inc.
July 2007

512.569.9760
steve.kramer@paragonscience.com
www.paragonscience.com

THE URGENT NEED

The United States faces a formidable asymmetric threat from diverse, global terrorist organizations. Unlike well-defined adversary states in previous conflicts such as the Cold War, present-day terrorist organizations are extremely difficult to counter because of their sparse, distributed, and adaptive nature.[1] They are typically organized in small covert cells designed to minimize the possibility of detection.[2,3]

Over the last several years, social network analysis and other graph-based technologies have been brought to bear on the problem of detecting covert terrorist networks.[4,5,6,7,8] These efforts have yielded positive results, but the current sets of techniques and tools still have significant shortcomings. A considerable number of existing approaches cannot simultaneously:

- Account for missing or erroneous data
- Model dynamic changes in network structure
- Model key flows and identify key players

In addition to the limitations noted above, many of the existing methods are too computationally expensive to be applied to the large, real-world data sets that must be analyzed in order to prevent terrorist attacks. In the TANGRAM proposal solicitation,[9] the Air Force Research Laboratory noted that "guilt by association" methods often fall short without an initially known suspect, which is a crucial consideration in counter-terrorism efforts.

A NEW SOLUTION

We have developed a patent-pending technique that explicitly addresses the needs cited above. Our algorithms are currently embodied in the form of the Paragon Network Analysis (PNA) software. Our method is more robust to missing or erroneous data than earlier techniques, especially those based on traditional centrality measures[10] or on subgroup connectivity.[8] Those previous approaches can be very sensitive to the omission of even a few key links, or edges, in a network.[11]

Unlike many existing methods, the PNA algorithms directly incorporate time-dependent data about communication events in order to characterize the dynamical evolution of a network. The time ordering of events is used explicitly in our formalism. Our initial tests indicate that our algorithms can track the changes in a terrorist cell as it transitions from a covert "sleeper" state to an active state.[6] Therefore, our software could aid the intelligence community by warning of impending attacks from covert cells going into action.

The PNA method employs a set of novel, dynamic network measures that can effectively identify covert terrorist cells and characterize their behavior over time. In this non-proprietary white paper, these parameters are referred to as α and β. Full details about the definitions of these new measures can be made available upon execution of an appropriate non-disclosure agreement. The PNA program uses several adjustable parameters, which can fine-tune the algorithm's ability to detect patterns of mediated communications. One important advantage of our method is that it does not require any *a priori* information about which entities to track; no "guilt by association" assumption is necessary.

Our technique promises to be scalable to large networks. Unlike centrality-based approaches that typically must solve the computationally expensive "all pairs, shortest distance" problem,[12] our method uses a purely local analysis that is highly parallelizable. Its basic computation time scales as $O(n\,k^2)$, where n is the number of nodes and k is the average degree for the network. Moreover, our software can effectively analyze streaming communications or transaction data. Unlike a number of previous techniques that must recalculate quantities over the entire graph at each time interval, only new and updated nodes need to be analyzed in the streaming-data scenario.

Our approach does not require any message content to detect anomalous behavior that might be indicative of covert terrorist networks; records of who contacted whom and when are sufficient. However, if message content is available, it can be used to filter communication events by assessing message similarity. Other filtering conditions can also be applied. For example, one could limit the analysis to communication events involving at least one contact outside the United States or those involving one or more agents on a watch list of known or suspected terrorists. Such filtering conditions can be used in concert with the PNA tunable parameters to winnow initial sets of anomalies down to fewer cases that meet the conditions of one or more threat signatures. These tools serve to decrease the likelihood of false positives.

PROMISING INITIAL RESEARCH RESULTS

We performed a number of tests using simulated communication events to test the PNA software's ability to detect patterns of mediated communications associated with covert terrorist cells in a "sleeper" state. Figure 1 is a graph that displays one example of how different types of simulated social networks can be readily distinguished by their respective positions when plotted according to their values of α and β. The results in the graph are for networks[13] of the following types, each consisting of 50 nodes:

- Erdos and Rényi (ER) random graphs[14] of 50 nodes with values of the uniform node linking probability ranging from 0.1 to 1.0
- Small-world networks[15] of 50 nodes with the rewiring probability ranging from 0.0 to 1.0
- Small-world networks of 45 nodes and one covert cell of 5 nodes, including a single mediator node
- Small-world networks of 40 nodes and two covert cells of 5 nodes, each including a single mediator node

In the simulations noted above, all communications within each covert cell flow through that cell's mediator node. Note that there is a clear separation between the "normal" networks without mediated communications and the networks containing covert terrorist cells that use mediated communications. The calculations for Figure 1 were for networks of 50 nodes. Our software has also successfully detected four covert cells that each consist of only 5 nodes and that are embedded in larger networks, up to 1,000,000 nodes in our initial tests, and with no appreciable degradation in detection ability.

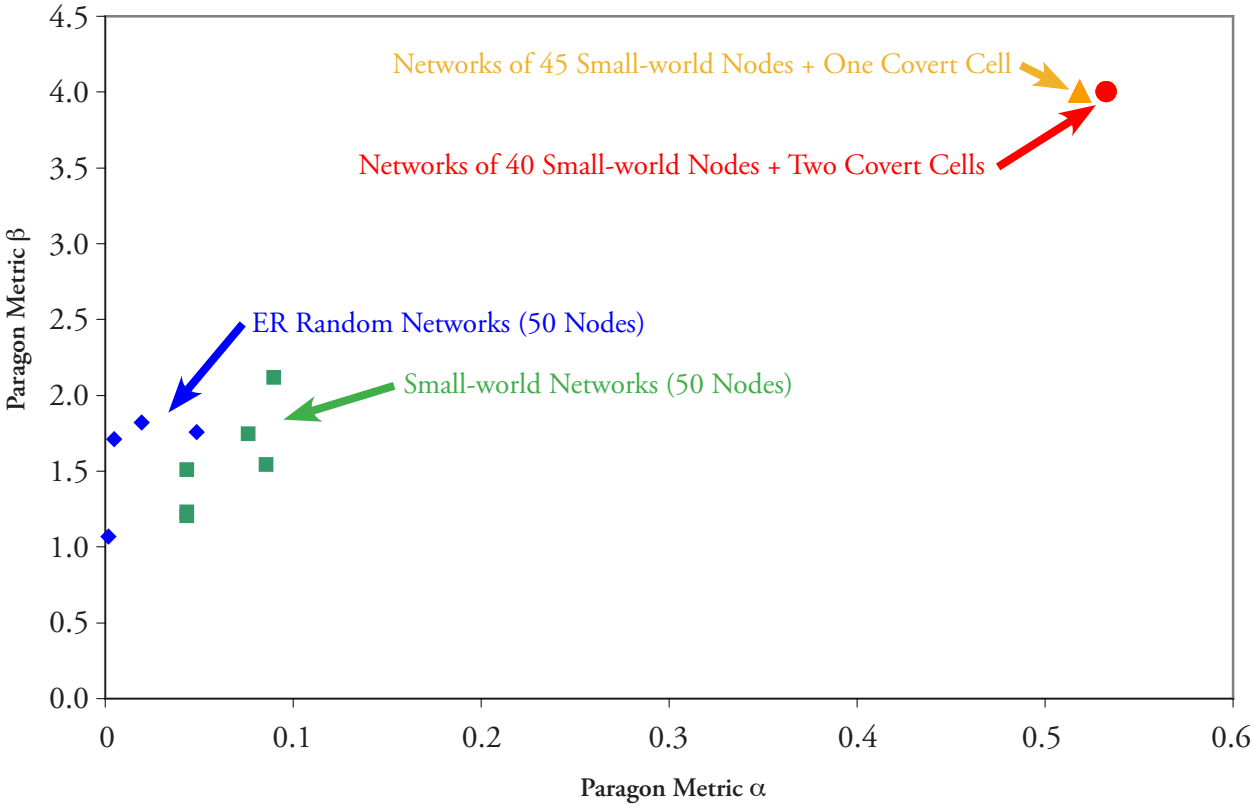

Figure 1. Paragon Metrics α and β for Different Network Types

The results of Figure 1 reflect the average parameter values over the entire time period that spans all of the communication events analyzed. To assess our method's ability to track the evolution of network communications patterns over time, we performed a second set of calculations in a sliding-time-window analysis. As input for these calculations, the event generator simulated communications within a covert cell that starts in a "sleeper" state with purely mediated communications, transitions to an active state with no mediation to prepare for an attack, and then switches back to the "sleeper" state.

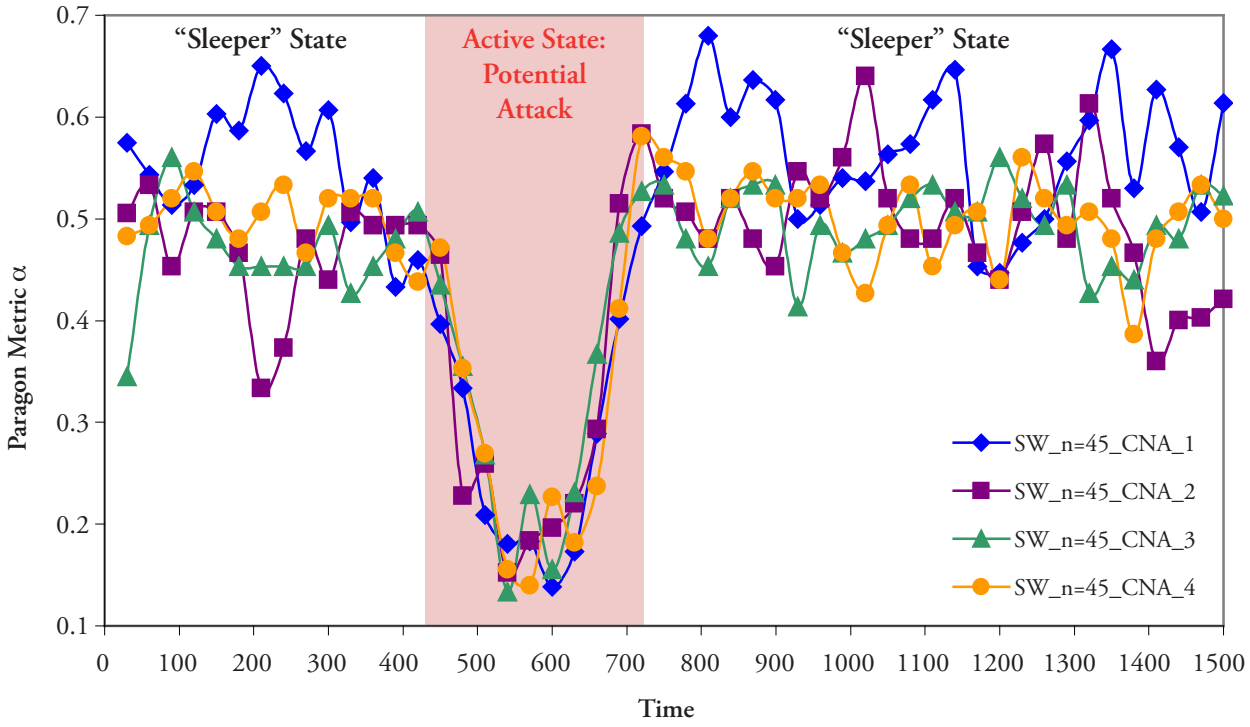

Figure 2. Paragon Metric α vs. Time for Networks of 45 Small-world Nodes and One Covert Cell

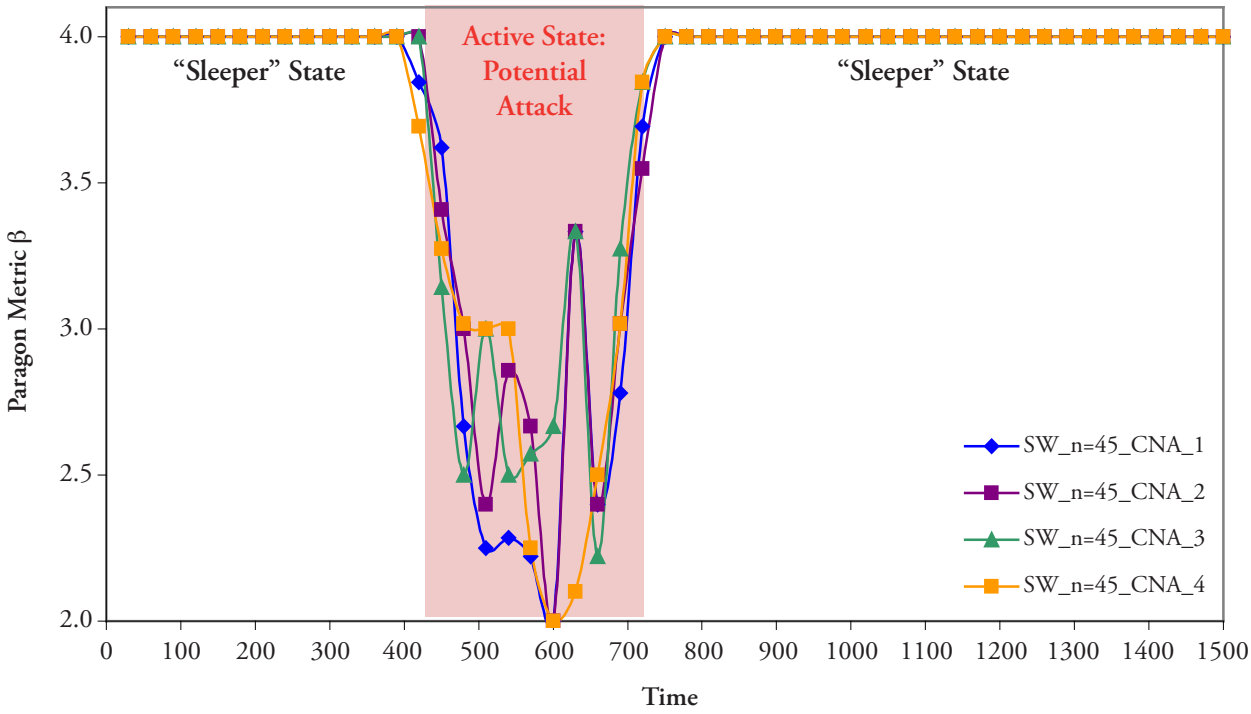

Figure 3. Paragon Metric β vs. Time for Networks of 45 Small-world Nodes and One Covert Cell

Figures 2 and 3 display the results for the mode-switching simulations for four different realizations of the numerical experiment. Figures 2 and 3 show α and β as functions of time, respectively. For both of these network parameters, the transition from the "sleeper" state to the active state and back is clearly visible. Thus, an automated system that uses the PNA program could monitor covert cells and warn intelligence analysts when the cells begin to switch to active mode.

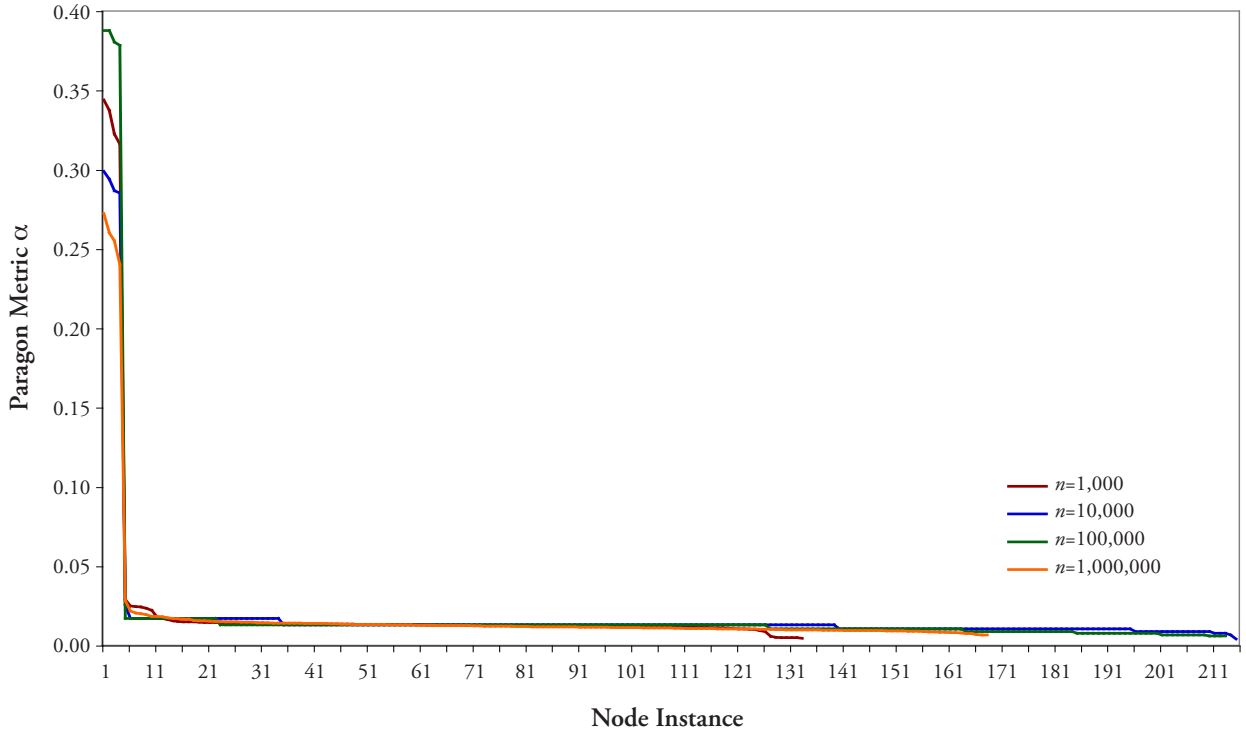

Figure 4. Leading Values of Paragon Metric α

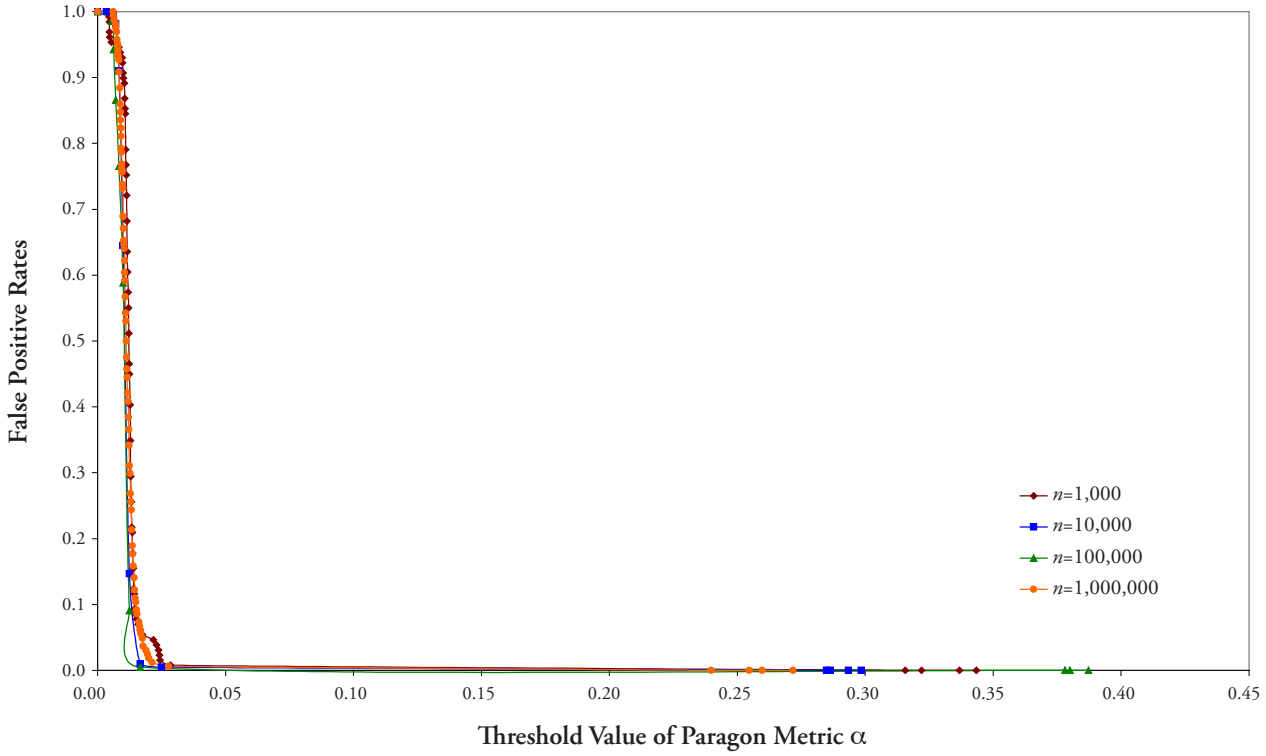

Figure 5. False Positive Rates

Figures 4 and 5 relate to scalability tests in which four covert cells of five terrorists each were embedded in small-world networks consisting of 10^3, 10^4, 10^5, and 10^6 nodes. Each terrorist was also connected to the surrounding small-world network and communicated with four non-terrorist neighbors with the same frequency as in the rest of the surrounding network. The largest calculation to date involved ~40M simulated communications.

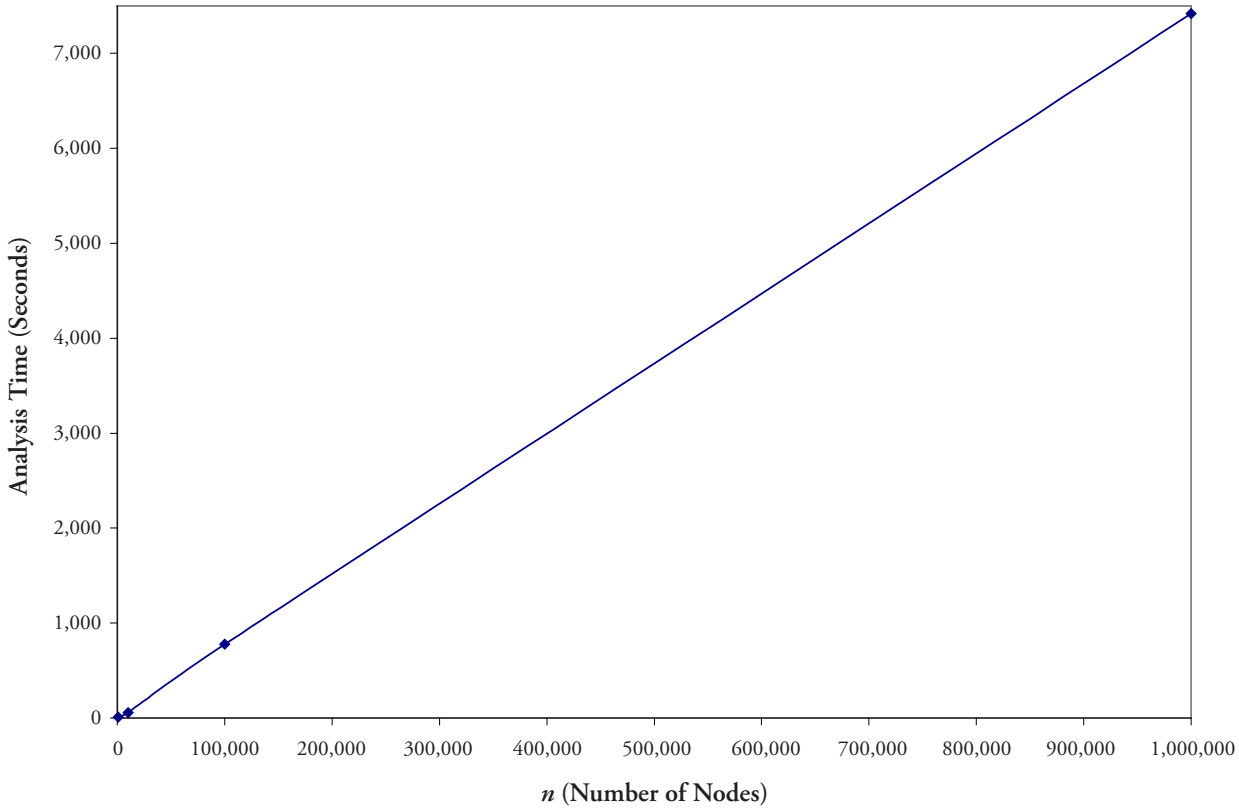

Figure 6. Analysis Time as a Function of Network Size

In all of these cases, the four leaders of the covert cells were clearly identified, as shown in Figure 4. Figure 5 shows the false positive rate (FPR)[16] as a function of the threshold value of Paragon metric α above which a node would be classified as a terrorist. The FPR rapidly drops to 0, well before the values of α associated with the terrorist leaders.

In order to check for the occurrence of false alarms on real-world communications data, we ran our software on the Reality Mining cell phone data set collected by Dr. Nathan Eagle at the MIT Media Lab.[17] In that study, the cell phone calling patterns of 100 volunteers were recorded for a period of a little longer than one year. Throughout the anticipated range of one of the key tunable parameters, there were no false positives generated.

As noted above, the computation time of our analysis algorithm scales as $O(n\,k^2)$. Figure 6 displays the analysis time as a function of network size n, the number of nodes. These calculations were performed on an Apple MacBook Pro notebook computer with 2 GB of RAM and a 2.1-GHz Intel Core 2 Duo processor.

Finally, our method is robust to the omission of even a relatively large percentage of captured network traffic. In one set of observability tests, the PNA software was able to identify the anomalous terrorist cells even when up to 90% of the full input data set was omitted. This characteristic is particularly advantageous because real-world data about covert networks must be assumed to be incomplete and uncertain.

NEXT STEPS

The initial research results presented above demonstrate that our novel approach could be a valuable tool for the United States in its counter-terrorism efforts. We welcome the opportunity to hone our algorithms to meet the needs of the United States Government. We look forward to working with potential partners and contract sponsors to define one or more challenging research and development projects.

BRIEF BIOGRAPHY OF DR. STEVE KRAMER

Dr. Steve Kramer is the President and Chief Scientist of Paragon Science, Inc. Drawing upon his research and consulting experience in the academic, business, and government fields, Dr. Kramer sets the research and business directions for the company. He founded Paragon Science with the goal of developing cutting-edge technologies to aid in the counter-terrorism efforts of the United States.

A native of Los Alamos, New Mexico, he worked during six summers at Los Alamos National Laboratory in the Computing Division and the Applied Theoretical Physics Division. In May 1987, he graduated *summa cum laude* with a B.A. in physics and mathematics from Trinity University in San Antonio, Texas, where he earned membership in Phi Beta Kappa. Working under Prof. Michael Marder in the Center for Nonlinear Dynamics at the University of Texas at Austin, he earned his Ph.D. in physics in May 1993. His dissertation on nonlinear models of rivers and river networks involved pattern formation in complex systems; computational physics; numerical solutions of nonlinear partial differential equations; and visualization of three-dimensional, time-dependent data. During graduate school, he was selected to attend the Complex Systems Summer School sponsored by the Santa Fe Institute.

From 1993 to 1997, he worked under Dr. Paul Rudolf at Forward Vision in San Antonio, Texas. During multiple SBIR contracts for the United States Air Force, Dr. Kramer performed research in computational electromagnetics; computer simulations of imaging systems and optical scanning devices; and numerical calculations of wave propagation applied to radar cross sections, inverse scattering, and interactions of microwaves with biological media.

From 1997 to 2001, Dr. Kramer worked in the e-commerce software industry. As Vice President of Education at Trilogy Software, he led a team of 25 people and oversaw a $1.3M annual budget to deliver technical training and technical documentation to external clients and internal employees. Following his years at Trilogy, he served as Manager of Educational Services at Motive Communications, another software company.

In 2002, combining his business and scientific knowledge, he began working to commercialize a new pattern recognition technology that Dr. Rudolf had invented. Since 2004, Dr. Kramer has also acted as a consultant to five Austin software companies. In 2005, he started his current research in graph theory, network analysis, and complex systems theory, yielding Paragon's counter-terrorism technology.

PUBLICATIONS

- P. Rudolf, S. Kramer, and J. Baxendale, "A software bridge to connect the USAF SRI (Scanning Radiometric Imager) to a model of the eye," SBIR Phase I Final Report, December 1995.
- P. Rudolf, S. Kramer, and J. Baxendale, "Spatial inverse scattering: theory and applications," SBIR Phase II Final Report, November 1995.
- P. Rudolf, S. Kramer, J. Baxendale, and C. Crump, "Virtual optics — a numerical imaging technique," SBIR Phase I Final Report, May 1994.
- Stephen P. Kramer, "Nonlinear models of rivers and river networks," doctoral dissertation, The University of Texas at Austin, May 1993.
- S. Kramer and M. Marder, "Evolution of river networks," *Phys. Rev. Lett.*, Vol. 68, pp. 205-208, 1992.
- R. E. H. Clark, J. Abdallah, Jr., G. Csanak, and S. P. Kramer, "Electron-impact cross sections and coherence parameters for the 6s2 1S - 6s 6p 1P transition in neutral barium," Phys. Rev. A, Vol. 40, pp. 2935–2949, 1989.

REFERENCES

[1] Rebecca Goolsby, "Computational Social Science, Culture and the Global War on Terror," Office of Naval Research Presentation [http://www.onr.navy.mil/about/conferences/rd_partner/2005/docs/past/2005/0507_goolsby_computational_social_science_culture_gwt.pdf], 2005.

[2] Kathleen M. Carley, "Estimating Vulnerabilities in Large Covert Networks," in *Proc. of the 9th International Command and Control Research and Technology Symposium*, Coronado Resort, CA, 2004.

[3] Maksim Tsvetovat and Kathleen M. Carley, "Generation of Realistic Social Network Datasets for Testing of Analysis and Simulation Tools," *Carnegie-Mellon University Technical Report CMU-ISRI-05-130*, 2005.

[4] T. Coffman, S. Greenblatt, S. Marcus, "Graph-Based Technologies for Intelligence Analysis," Communications of the ACM, *Special Issue on Emerging Technologies for Homeland Security*, Vol. 47, No. 3, pp. 45-47, March 2004.

[5] T. Coffman, S. Marcus, "Pattern Classification in Social Network Analysis: A Case Study," *Proc. 2004 IEEE Aerospace Conference*, Big Sky, MT, March 2004.

[6] T. Coffman, S. Marcus, "Dynamic Classification of Groups Through Social Network Analysis and HMMs," *Proc. 2004 IEEE Aerospace Conference*, Big Sky, MT, March 2004.

[7] M. Mukherjee and L. Holder, "Graph-Based Data Mining on Social Networks," *Workshop on Link Analysis and Group Detection (LinkKDD2004)*, 2004.

[8] J. Baumes, M. Goldberg, M. Magdon-Ismail, and A. Wallace, "Discovering Hidden Groups in Communication Networks," in *Proc. of the 2nd NSF/NIJ Symposium on Intelligence and Security Informatics*, 2004.

[9] Air Force Research Laboratory, TANGRAM Proposer Information Packet, 2005.

[10] S. Borgatti, "Centrality and Network Flow," *Social Networks*, Vol. 27, No. 1, pp. 55-71, 2005.

[11] Valdis E. Krebs, "Mapping Networks of Terrorist Cells," *Connections*, Vol. 24, No. 3, pp.43-52, 2002.

REFERENCES

[12] Ulrik Brandes, "A Faster Algorithm for Betweenness Centrality," *Journal of Mathematical Sociology*, Vol. 25, No. 2, pp. 163-177, 2001.

[13] The random graphs and small-world networks used as input for the initial calculations up to n=1000 were generated by the SpectralNET application developed by the Broad Institute of MIT and Harvard. We gratefully acknowledge the assistance of Dr. Stephen Haggarty. For more information, refer to J. Forman, P. Clemons, S. Schreiber, and S. Haggarty, "SpectralNET – An Application for Spectral Graph Analysis and Visualization," *BMC Bioinformatics*, Vol. 6, pp. 260-260, 2005.

[14] P. Erdos and A. Renyi, "On the Evolution of Random Graphs," *Publ. Math. Inst. Hungar. Acad. Sci.*, pp. 17-61, 1960.

[15] D. J. Watts and S. H. Strogatz, "Collective Dynamics of 'Small-World' Networks," *Nature*, Vol. 393, pp. 440-442, 1998.

[16] The FPR curves were calculated using modifications to ROC software graciously provided by Dr. Tom Fawcett. For more details, refer to Tom Fawcett, "ROC Graphs: Notes and Practical Considerations for Researchers," HP Labs Tech Report HPL-2003-4 (http://www.purl.org/net/tfawcett/papers/ROC101.pdf), 2003.

[17] N. Eagle and A. Pentland,"Reality Mining: Sensing Complex Social Systems," *Personal and Ubiquitous Computing*, Vol. 10, No. 4, 2006. We thank Dr. Eagle for making his data available to us.