REPORT DOCUMENTATION PAGE

Form Approved OMB NO. 0704-0188

1. REPORT DATE (DD-MM-YYYY)	2. REPORT TYPE	3. DATES COVERED (From - To)
25-09-2014	Final Report	8-May-2007 - 30-Jun-2013

4. TITLE AND SUBTITLE
Designing Robust and Resilient Tactical MANETs

5a. CONTRACT NUMBER
W911NF-07-1-0287

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER
611103

6. AUTHORS
Virgil Gligor, John Baras, Jonathan Katz, Carlos Guestrin, Adrian Perrig, Rohit Negi, Radha Poovendran, James Ritchey, Nitin Vaidya, R. Srikant, P.R. Kumar, Yih-Chu Hu

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAMES AND ADDRESSES
University of Maryland - College Park
3112 Lee Building

College Park, MD 20742 -5141

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS (ES)
U.S. Army Research Office
P.O. Box 12211
Research Triangle Park, NC 27709-2211

10. SPONSOR/MONITOR'S ACRONYM(S)
ARO

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
52567-CS-MUR.3

12. DISTRIBUTION AVAILIBILITY STATEMENT
Approved for Public Release; Distribution Unlimited

13. SUPPLEMENTARY NOTES
The views, opinions and/or findings contained in this report are those of the author(s) and should not contrued as an official Department of the Army position, policy or decision, unless so designated by other documentation.

14. ABSTRACT
The overall research theme of this MURI, is the design and operation of reliable and secure tactical MANET. The emphasis of this research is the discovery and development of methods and algorithms that can unify the investigation of resiliency and security for MANETs. With this emphasis, we investigate fundamental problems addressing the characterization, properties and design of the Trusted Core of a MANET. More specifically we investigated several research problems in the context of four broad thrusts, namely (1) Design of the Trusted Core, (2) Adaptive Protocol Monitoring for Efficiency and Dependability, (3)Network Utility Maximization, and Threat

15. SUBJECT TERMS
Wireless Networks, tactical networks, MANETs, Resilience, Robustness,

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	15. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Virgil Gligor
UU	UU	UU	UU		19b. TELEPHONE NUMBER 412-268-9833

Report Title

Designing Robust and Resilient Tactical MANETs

ABSTRACT

The overall research theme of this MURI, is the design and operation of reliable and secure tactical MANET. The emphasis of this research is the discovery and development of methods and algorithms that can unify the investigation of resiliency and security for MANETs. With this emphasis, we investigate fundamental problems addressing the characterization, properties and design of the Trusted Core of a MANET. More specifically we investigated several research problems in the context of four broad thrusts, namely (1) Design of the Trusted Core, (2) Adaptive Protocol Monitoring for Efficiency and Dependability, (3)Network Utility Maximization, and Threat Modeling Detection and Defense in MANETs

Enter List of papers submitted or published that acknowledge ARO support from the start of the project to the date of this printing. List the papers, including journal references, in the following categories:

(a) Papers published in peer-reviewed journals (N/A for none)

Received	Paper
09/25/2014 23.00	Kyoung-Dae Kim, P. R. Kumar. A Real-Time Middleware for Networked Control Systems and Application to an Unstable System, IEEE Transactions on Control Systems Technology, (01 2012): 0. doi:
09/25/2014 24.00	Kyoung-Dae Kim, P. R. Kumar. Cyber-Physical Systems: A Perspective at the Centennial, Proceedings of the IEEE: Centennial Issue, (05 2012): 1287. doi:
09/25/2014 10.00	E. Athanasopoulou, L. Bui, T. Ji, R. Srikant, A. L. Stolyar. Back-Pressure-Based Packet-by-Packet Adaptive Routing in Communication Networks, IEEE/ACM Transactions on Networking, (01 2012): 0. doi:
09/25/2014 11.00	G. Theodorakopoulos , J. S. Baras. Game Theory Modeling of Malicious Users in Collaborative Networks, IEEE Journal on Selected Areas in Communications, Special Issue on Game Theory in Communication Systems, (09 2008): 1317. doi:
09/25/2014 12.00	H. Kowshik, Derek Caveney, P.R. Kumar. Provable Systemwide Safety in Intelligent Intersections, IEEE Transactions on Vehicular Technology, (03 2011): 804. doi:
09/25/2014 13.00	Haowen Chan, Hsu-Chun Hsiao, Adrian Perrig, Dawn Song. Secure Distributed Data Aggregation, Foundations and Trends in Databases, (01 2011): 149. doi:
09/25/2014 14.00	P. R. Kumar, Hemant Kowshik. Optimal Function Computation in Directed and Undirected Graphs, IEEE TRANSACTIONS ON INFORMATION THEORY, (06 2012): 3407. doi:
09/25/2014 15.00	I-Hong Hou, P. R. Kumar. Queueing Systems with Hard Delay Constraints: A Framework and Solutions for Real-Time Communication over Unreliable Wireless Channels, Queueing Systems: Theory and Applications, (01 2012): 151. doi:
09/25/2014 16.00	I-Hong Hou, P. R. Kumar. Real-Time Communication over Unreliable Wireless Links: A Theory and Its Applications, IEEE Wireless Communications Magazine, (01 2012): 48. doi:
09/25/2014 19.00	J. Ni, R. Srikant, X. Wu. Coloring Spatial Point Processes with Applications to Peer Discovery in Large Wireless Networks, IEEE/ACM Transactions on Networking, (01 2011): 0. doi:
09/25/2014 17.00	J. Ghaderi, R. Srikant. The Impact of Access Probabilities on the Delay Performance of Q-CSMA Algorithms in Wireless Networks, IEEE/ACM Transactions on Networking, (2012): 0. doi:
09/25/2014 18.00	B. Tan, J. Ni, R. Srikant. Q-CSMA: Queue-Length-Based CSMA/CA Algorithms for Achieving Maximum Throughput and Low Delay in Wireless Networks, IEEE/ACM Transactions on Networking, (06 2012): 0. doi:
09/25/2014 20.00	J. S. Baras. Security and Trust for Wireless Autonomic Networks: System and Control Methods, European Journal of Control: Special Issue, (03 2007): 105. doi:
09/25/2014 21.00	Jerry T. Chiang, Jason J. Haas, Jihyuk Choi, Yih-Chun Hu. Secure Location Verification Using Simultaneous Multilateration, IEEE Transactions on Wireless Networking , (02 2012): 584. doi:

09/25/2014 22.00 Radha Poovendran, Krishna Sampigethaya, Sudhakar Shetty, Terry Davis, Chuck Royalty. Future e-enabled aircraft communications and security: The next twenty years and beyond,
Proceedings of the IEEE, Special issue on Aerospace Communications and Networking in the Next Two Decades, (12 2011): 0. doi:

09/25/2014 25.00 M. Leconte, L. Jiang, J. Ni, R. Srikant, J. Walrand. Fast Mixing of Parallel Glauber Dynamics and Low-Delay CSMA Scheduling,
IEEE TRANSACTIONS ON INFORMATION THEORY, (10 2012): 0. doi:

09/25/2014 26.00 M. Leconte, J. Ni, R. Srikant. Improved Bounds on the Throughput Efficiency of Greedy Maximal Scheduling in Wireless Networks,
IEEE/ACM Transactions on Networking, (06 2011): 0. doi:

09/25/2014 27.00 N. Freris, H. Kowshik, P.R. Kumar. Fundamentals of Large Sensor Networks: Connectivity, Capacity, Clocks and Computation,
Proceedings of the IEEE, (11 2010): 1828. doi:

09/25/2014 28.00 P. Purkayastha, J.S. Baras. An Optimal Distributed Routing Algorithm using Dual Decomposition Techniques,
Communications in Information and Systems, Brockett Legacy Issue, International Press, (12 2008): 277. doi:

09/25/2014 29.00 Patrick Tague, David Slater, Jason Rogers, Radha Poovendran. Evaluating the Vulnerability of Network Traffic Using Joint Security and Routing Analysis,
IEEE Transactions on Dependable and Secure Computing, (04 2009): 111. doi:

09/25/2014 30.00 Patrick Tague, Mingyan Li, Radha Poovendran. Mitigation of Control Channel Jamming under Node Capture Attacks,
IEEE Transactions on Mobile Computing, (09 2009): 0. doi:

09/25/2014 31.00 Patrick Tague, Sidharth Nabar, Jim Ritcey, Radha Poovendran. Jamming-Aware Traffic Allocation for Multiple-Path Routing using Portfolio Selection,
IEEE/ACM Transactions on Networking, (02 2011): 0. doi:

09/25/2014 32.00 S. Zheng, J.S. Baras. Sequential Anomaly Detection in Wireless Sensor Networks and Effects of Long Range Dependant Data,
Special IWSM Issue of Sequential Analysis, (11 2012): 0. doi:

09/25/2014 4.00 A. D. Dominguez-Garcia, C. N. Hadjicostis, N. H. Vaidya. Resilient Networked Control of Distributed Energy Resources,
IEEE Journal on Selected Areas in Communications, (07 2012): 0. doi:

09/25/2014 5.00 Andreas Krause, Amarjeet Singh, Carlos Guestrin, William Kaiser . Efficient Informative Sensing using Multiple Robots,
Journal of Artificial Intelligence Research, (01 2009): 707. doi:

09/25/2014 6.00 Mark Luk, Adrian Perrig, Arvind Seshadri . SAKE: Software attestation for key establishment in sensor network,
Ad Hoc Networks Journal, (01 2011): 1059. doi:

09/25/2014 7.00 B. Alomair , R. Poovendran. E-MACs: Towards More Secure and More Efficient Constructions of Secure Channels,
IEEE Transactions on Computers, (01 2012): 0. doi:

09/25/2014 8.00 B. Alomair, A. Clark, J. Cuellar, R. Poovendran. Scalable RFID Systems: a Privacy-Preserving Protocol with Constant-Time Identification,
IEEE Trans. Parallel and Distributed Systems, (01 2012): 1536. doi:

09/25/2014 9.00 B. Alomair, A. Clark, J. Cuellar, R. Poovendran. Towards Statistical Framework for Source Anonymity in Sensor Networks,
IEEE Transactions on Mobile Computing , (01 2011): 0. doi:

09/25/2014 33.00 Girish Baliga, P. R. Kumar, Scott Graham. Abstractions, Architecture, Mechanisms, and a Middleware for Networked Control,
IEEE Transactions on Automatic Control, (07 2009): 1490. doi:

09/25/2014 34.00 T. Bonaci, P. Lee, L. Bushnell, R. Poovendran. A Convex Optimization Approach for Clone Detection in Wireless Sensor Networks,
Pervasive and Mobile Computing, (01 2012): 0. doi:

09/25/2014 35.00 Vivek Raghunathan, P. R. Kumar. Wardrop routing in wireless networks,
IEEE Transactions on Mobile Computing, (05 2009): 636. doi:

09/25/2014 36.00 W. Shi, J. Ritcey. Cooperative transmit and jamming for maximizing secrecy rate of Gaussian MISO wiretap channels,
IEEE Transactions on Communications, (01 2013): 0. doi:

09/25/2014 37.00 Yue-Hsun Lin, Ahren Studer, Yao-Hsin Chen, Hsu-Chun Hsiao, Li-Hsiang Kuo, Jason Lee, Jonathan M. McCune, King-Hang Wang, Maxwell Krohn, Phen-Lan Lin, Adrian Perrig, Hung-Min Sun, Bo-Yin Yang.
SPATE: Small-Group PKI-Less Authenticated Trust Establishment,
IEEE Transactions on Mobile Computing , (12 2010): 0. doi:

TOTAL: **34**

Number of Papers published in peer-reviewed journals:

(b) Papers published in non-peer-reviewed journals (N/A for none)

Received Paper

TOTAL:

Number of Papers published in non peer-reviewed journals:

(c) Presentations

A. Clark, L. Bushnell, R. Poovendran, Joint Leader and Link Weight Selection for Fast Convergence in Multi-Agent Systems, submitted to IEEE ACC 2013.

A. Clark, Q. Zhu, R. Poovendran, T. Basar, "An Impact-Aware Defense against Stuxnet," submitted to IEEE ACC 2013.

Anand Muralidhar and P. R. Kumar, "Near-optimal quantization and linear network coding for relay networks," Submitted to IEEE Transactions on Information Theory. Submitted March 11, 2012.

G. Theodorakopoulos, J-Y. Le Boudec and J. S. Baras, "Selfish Response to Epidemic Propagation", accepted for publication in the IEEE Transactions on Automatic Control, to be published, February 2013.

Hemant Kowshik and P. R. Kumar, "Optimal Computation of Symmetric Boolean Functions in Col- located Networks." Submitted to IEEE Journal on Selected Areas in Communications: In-Network Computation: Exploring the Fundamental Limits. Submitted February 22, 2012.

I. Matei, J.S. Baras and V. Srinivasan, "Trust-Based Multi-Agent Filtering for Increased Smart Grid Security," journal paper, submitted, August 2012.

J.S. Baras and T. Jiang, "Composite Trust in Networked Multi-Agent Systems", journal paper, submitted, June 2012.

Jonathan Katz and Yehuda Lindell, Aggregate Message Authentication Codes, IET Proc. Information Security. Accepted pending revisions.

Kyoung-Dae Kim, Sayan Mitra and P. R. Kumar, "Bounded ?-Reach Set Computation of a Class of Deterministic and Transversal Linear Hybrid Automata." Submitted to IEEE Transactions on Automatic Control. May 15, 2012.

L. Tseng and N. H. Vaidya, "Iterative Approximate Byzantine Consensus under a Generalized Fault Model," to appear at International Conference on Distributed Computing and Networking (ICDCN), India, January 2013.

N. H. Vaidya, C. N. Hadjicostis, A. D. Dominguez-Garcia, "Robust Average Consensus over Packet Dropping Links: Analysis via Coefficients of Ergodicity," to appear at IEEE Control and Decision Conference, 2012.

Q. Zhu, A. Clark, R. Poovendran, T. Basar, SODEXO: A System Framework for Deployment and Exploitation of Deceptive Honeybots in Social Networks, under review at INFOCOM'2013.

S. Dov Gordon, Jonathan Katz, Ranjit Kumaresan, and Arkady Yerukhimovich. Authenticated Broadcast with a Partially Compromised Public-Key Infrastructure, Invited to a special issue of Information & Computation. Awaiting publication.

T. H. Kim, J. Ni, R. Srikant and N. H. Vaidya, "On the achievable throughput of CSMA under imperfect carrier sensing," IEEE/ACM Transactions on Networking (under review).

T. Jiang and J.S. Baras, "Collaboration in Networked Systems and Trust", journal paper, submitted, May 2012.

Tae Hyun Kim, Jian Ni, R. Srikant, N. H. Vaidya, "Throughput-Optimal CSMA with Imperfect Carrier Sensing," submitted to the IEEE/ACM Transactions on Networking

Number of Presentations: 16.00

Non Peer-Reviewed Conference Proceeding publications (other than abstracts):

Received	Paper

TOTAL:

Number of Non Peer-Reviewed Conference Proceeding publications (other than abstracts):

Peer-Reviewed Conference Proceeding publications (other than abstracts):

Received		Paper
09/25/2014	38.00	A. Clark, L. Bushnell, R. Poovendran, . Leader Selection for Minimizing Convergence Error in Leader-Follower Systems: A Supermodular Optimization Approach, Wiopt'12. 14-MAY-12, . : ,
09/25/2014	39.00	A. Clark, Q. Zhu, R. Poovendran, T. Basar. Deceptive Routing in Relay Networks, GameSec. 01-NOV-12, . : ,
09/25/2014	40.00	R. Poovendran, A. Clark. A submodular Optimization Framework for Leader Selection in Linder Multi-Agent Systems, IEEE CDC. 01-DEC-11, . : ,
09/25/2014	41.00	A. Roy-Chowdhury, J. S. Baras. Probabilistic Non-Repudiation for Source Authentication with TESLA Certificates in Hybrid Satellite/Wireless and Performance Analysis of the Authentication Protocol, Ka and Broadband Communications Conference Navigation and Earth Observation Conference. 23-SEP-09, . : ,
09/25/2014	42.00	Ahren Studer, Adrian Perrig. Mobile User Location-specific Encryption (MULE): Using Your Office as Your Password, ACM Conference on Wireless Network Security (WiSec). 01-MAR-10, . : ,
09/25/2014	43.00	Ahren Studer, Adrian Perrig. The Coremelt Attack, European Symposium on Research in Computer Security (ESORICS). 01-SEP-09, . : ,
09/25/2014	44.00	Amit Vasudevan, Bryan Parno, Ning Qu, Virgil D. Gligor, Adrian Perrig. Lockdown: Towards a Safe and Practical Architecture for Security Applications on Commodity Platforms, 5th International Conference on Trust and Trustworthy Computing (TRUST). 01-JUN-12, . : ,
09/25/2014	45.00	Andreas Krause, Ram Rajagopal, Anupam Gupta, Carlos Guestrin . Simultaneous Placement and Scheduling of Sensors, Information Processing in Sensor Networks (IPSN). 01-JAN-09, . : ,
09/25/2014	46.00	Andrew Clark, Rommie Hardy, Radha Poovendran. A Joint Performance-Vulnerability Metric Framework for Designing Ad Hoc Routing Protocols, IEEE Military Communications Conference (MILCOM '10) . 01-NOV-10, . : ,
09/25/2014	47.00	Bryan Parno, Jonathan M. McCune, Adrian Perrig. Bootstrapping Trust in Commodity Computers, IEEE Symposium on Security and Privacy. 01-MAY-10, . : ,
09/25/2014	48.00	Bryan Parno, Zongwei Zhou, Adrian Perrig. Using Trustworthy Host-Based Information in the Network, 7th ACM Workshop on Scalable Trusted Computing (STC). 01-OCT-12, . : ,
09/25/2014	49.00	C. L. Robinson, P. R. Kumar. Networked Control Systems with Packet Delays and Losses, 47th IEEE Conference on Decision and Control. 09-DEC-08, . : ,
09/25/2014	50.00	C. Yang, B. Alomair, R. Poovendran. Multipath Flow Allocation in Anonymous Wireless Networks with Dependent Sources, 50th Allerton Conference. 01-OCT-12, . : ,

09/25/2014 51.00 C. Yang, B. Alomair, R. Poovendran. Optimized Flow Allocation for Anonymous Communication in Multipath Wireless Network,
IEEE ISIT 2012. 01-JUL-12, . : ,

09/25/2014 52.00 Tzong-Chen Wu, Chia-Hsin Owen Chen, Chung-Wei Chen, Cynthia Kuo, Yan-Hao Lai, Jonathan M. McCune , Ahren Studer, Adrian Perrig, Bo-Yin Yang. GAnGS: Gather Authenticate 'n Group Securely,
ACM Annual International Conference on Mobile Computing and Networking (MobiCom). 01-SEP-08, . : ,

09/25/2014 53.00 Dafna Shahaf, Anton Chechetka, Carlos Guestrin . Learning Thin Junction Trees via Graph Cuts,
In Artificial Intelligence and Statistics (AISTATS). 01-JAN-09, . : ,

09/25/2014 54.00 Dan Boneh, David Freeman, Brent Waters . Signing a Linear Subspace: Signatures for Network Coding,
Public-Key Cryptography (PKC). 01-JAN-09, . : ,

09/25/2014 55.00 David Slater, Patrick Tague, Radha Poovendran, Brian J. Matt. A Coding-Theoretic Approach for Efficient Message Verification Over Insecure Channels,
Second ACM Conference on Wireless Network Security (WiSec) . 01-MAR-09, . : ,

09/25/2014 58.00 Dongwon Seo, Heejo Lee , Adrian Perrig. PFS: Probabilistic Filter Scheduling Against Distributed Denial-of-Service Attacks,
IEEE Conference on Local Computer Networks (LCN). 01-JAN-11, . : ,

09/25/2014 59.00 Farhana Ashraf, Yih-Chun Hu, Robin H. Kravets. Bankrupting the Jammer in WSN,
9th IEEE International Conference on Mobile Ad-hoc and Sensor Systems (MASS 2012). 01-OCT-12, . : ,

09/25/2014 60.00 N. H. Vaidya, G. Liang. Capacity of Byzantine Consensus in Capacity Limited Point-to-Point Networks,
4th International Conference on COMmunication Systems and NETworkS (COMSNETS). 01-JAN-12, . : ,

09/25/2014 56.00 Deepayan Chakrabarti, Jure Leskovec, Christos Faloutsos, Samuel Madden, Carlos Guestrin, Michalis Faloutsos. Information Survival Threshold in Sensor and P2P Networks,
INFOCOM. 01-JAN-07, . : ,

09/25/2014 61.00 N. H. Vaidya, G. Liang . Capacity of Byzantine Agreement with Finite Link Capacity,
IEEE INFOCOM. 01-APR-11, . : ,

09/25/2014 57.00 Yih-Chun Hu, Dongho Kim. A Study on False Channel Condition Reporting Attacks in Wireless Networks,
Sixth International ICST Conference on Security and Privacy in Communication Networks (SecureComm 2010). 01-SEP-10, . : ,

09/25/2014 62.00 G. Liang , N. H. Vaidya. Error-Free Multi-Valued Consensus with Byzantine Failures,
ACM PODC. 01-JUN-11, . : ,

09/25/2014 63.00 G. Taban , V.D. Gligor. Efficient Handling of Adversary Attacks in Aggregation Applications,
Proc. of the European Symp. on Research in Security and Privacy (ESORICS). 01-OCT-08, . : ,

09/25/2014 64.00 G. Theodorakopoulos, J. S. Baras. Dynamic Network Security Deployment Under Partial Information,
Forty-Sixth Annual Allerton Conference on Communication, Control, and Computing. 23-SEP-08, . : ,

09/25/2014 65.00 G. Theodorakopoulos, J. S. Baras. Game Theory Modeling of Malicious Users in Collaborative Networks,
Journals on Selected Areas in Communications, Special Issue on Game Theory in Communication Systems. 01-SEP-08, . : ,

09/25/2014 66.00 Virgil Gligor, Adrian Perrig, Panos Papadimitratos, Ghita Mezzour. Privacy-Preserving Relationship Path Discovery in Social Networks,
International Conference on Cryptology and Network Security (CANS). 01-DEC-09, . : ,

09/25/2014 67.00 Nitin Vaidya, Guanfeng Liang . Byzantine Broadcast in Point-to-Point Networks using Local Linear Coding,
ACM Symposium on Principles of Distributed Computing (PODC). 01-JUL-12, . : ,

09/25/2014 68.00 Guanfeng Liang, Benjamin Sommer, Nitin Vaidya. Experimental Performance Comparison of Byzantine Fault-Tolerant Protocols for Data Centers,
IEEE INFOCOM . 01-JAN-12, . : ,

09/25/2014 69.00 Haowen Chan , Adrian Perrig. Efficient Security Primitives Derived from a Secure Aggregation Algorithm,
ACM Conference on Computer and Communications Security (CCS). 01-OCT-08, . : ,

09/25/2014 70.00 Haowen Chan, Adrian Perrig. Round-Efficient Broadcast Authentication Protocols for Fixed Topology Classes,
IEEE Symposium on Security and Privacy. 01-MAY-10, . : ,

09/25/2014 72.00 Hemant Kowshik, P. R. Kumar. Optimal computation of symmetric Boolean functions in Tree networks,
Proceedings of the 2010 IEEE International Symposium on Information Theory (ISIT 2010). 13-JUN-10, . : ,

09/25/2014 71.00 He Wu, Sidharth Nabar , Radha Poovendran. An Energy Framework for the Network Simulator 3 (ns-3), ,
4th International ICST Conference on Simulation Tools and Techniques (SIMUTools '11). 01-JAN-12, . : ,

09/25/2014 73.00 P. R. Kumar, Hemant Kowshik. Optimal ordering of transmissions for Boolean function computation.,
IEEE International Symposium on Information Theory (ISIT 2010). 13-JUN-10, . : ,

09/25/2014 74.00 Hemant Kowshik, P. R. Kumar. Optimal strategies for computing symmetric Boolean functions in collocated networks,
2010 IEEE Information Theory Workshop. 06-JAN-10, . : ,

09/25/2014 75.00 Hemant Kowshik , P. R. Kumar. Zero-error Function Computation in Sensor Networks,
48th IEEE Conference on Decision and Control. 16-DEC-09, . : ,

09/25/2014 76.00 Hemant Kowshik, Derek Caveney, P. R. Kumar. Safety and Liveness in Intelligent Intersections,
11th International Workshop, HSCC 2008. 22-APR-08, . : ,

09/25/2014 77.00 Hossen Mustafa, Xin Zhang, Zhenhua Liu, Wenyuan Xu, Adrian Perrig. Short Paper: Jamming-Resilient Multipath Routing Leveraging Availability-Based Correlation,
ACM Conference on Wireless Network Security (WiSec). 01-JUN-11, . : ,

09/25/2014 78.00 Hsu-Chun Hsiao, Ahren Studer, Chen Chen, Adrian Perrig, Fan Bai, Bhargav Bellur, Aravind Iyer. Flooding-Resilient Broadcast Authentication for VANETs,
ACM Annual International Conference on Mobile Computing and Networking (MobiCom). 01-SEP-11, . : ,

09/25/2014 79.00 Hsu-Chun Hsiao, Ahren Studer, Rituik Dubey, Elaine Shi, Adrian Perrig. Efficient and Secure Threshold-based Event Validation for VANETs,
ACM Conference on Wireless Network Security (WiSec). 01-JUN-11, . : ,

09/25/2014 80.00 I. Matei, J.S. Baras , T. Jiang. A Composite Trust Model and its Applications to Collaborative Distributed Information Fusion,
12th International Conference on Information Fusion-Fusion. 06-JUL-09, . : ,

09/25/2014 81.00 I. Matei, J.S. Baras , V. Srinivasan. Trust-Based Multi-Agent Filtering for Increased Smart Grid Security,
20th Mediterranean Conference on Control and Automation. 03-JUL-12, . : ,

09/25/2014 82.00 I-Hong Hou, P. R. Kumar. Admission Control and Scheduling for QoS Guarantees for Variable-Bit-Rate Applications on Wireless Channels,
MobiHoc 2009. 18-MAY-09, . : ,

09/25/2014 83.00 I-Hong Hou, P. R. Kumar. A Survey of Recent Results on Real-Time Wireless Networking,
Real-time Wireless for Industrial Applications, CPS Week. 11-APR-11, . : ,

09/25/2014 84.00 P. R. Kumar, I-Hong Hou . Admission Control and Scheduling for QoS Guarantees for Variable-Bit-Rate Applications on Wireless Channels,
MobiHoc 2009. 18-MAY-09, . : ,

09/25/2014 85.00 I-Hong Hou, P. R. Kumar. Broadcasting Delay-Constrained Traffic over Unreliable Wireless Links with Network Coding,
MobiHoc 2011. 16-MAY-11, . : ,

09/25/2014 86.00 I-Hong Hou, P. R. Kumar. Scheduling Heterogeneous Real-Time Traffic over Fading Wireless Channels,
Infocom 2010. 15-MAR-10, . : ,

09/25/2014 87.00 I-Hong Hou, P. R. Kumar. Utility Maximization for Delay Constrained QoS in Wireless,
Infocom 2010. 15-MAR-10, . : ,

09/25/2014 88.00 I-Hong Hou, V. Borkar, P. R. Kumar. A Theory of QoS for Wireless,
Infocom 2009. 19-APR-09, . : ,

09/25/2014 89.00 J. Ghaderi, R. Srikant. Flow-Level Stability of Multihop Wireless Networks Using Only MAC-Layer Information,
WiOpt 2012. 01-JAN-12, . : ,

09/25/2014 90.00 J. Ghaderi, R. Srikant. Effect of Access Probabilities on the Delay Performance of Q-CSMA Algorithms,
IEEE INFOCOM 2012. 01-JAN-12, . : ,

09/25/2014 91.00 J. Ghaderi, T. Ji, R. Srikant. Connection-Level Scheduling in Wireless Networks Using Only MAC-Layer Information,
IEEE INFOCOM 2012 Mini-Conference. 01-JAN-12, . : ,

09/25/2014 92.00 J. Katz , Y. Lindell. Aggregate Message Authentication Codes,
RSA 2008 . 01-JAN-08, . : ,

09/25/2014 93.00 J. Ni, Bo Tan, R. Srikant. Q-CSMA: Queue-Length Based CSMA/CA Algorithms for Achieving Maximum Throughput and Low Delay in Wireless Networks,
29th IEEE Conference on Computer Communications (INFOCOM) Mini-Conference. 01-MAR-12, . : ,

09/25/2014 94.00 R. Srikant, X. Wu, J. Ni. Coloring Spatial Point Processes with Applications to Peer Discovery in Large Wireless Networks,
12th ACM International Conference on Measurement and Modeling of Computer Systems (SIGMETRICS). 01-JUN-10, . : ,

09/25/2014 95.00 J. S. Baras, P. Hovareshti. Effects of Topology in Networked Systems: Stochastic Methods and Small Worlds,
Proceedings of the 47th IEEE Conference on Decision and Control. 09-DEC-08, . : ,

09/25/2014 96.00 P. Hovareshti , S. Perumal, J. S. Baras. Event Triggered Distributed Collaborative Control,
European Control Conference 2009 – ECC‘09. 23-AUG-09, . : ,

09/25/2014 97.00 J. S. Baras, T. Jiang , P. Hovareshti. Coalition Formation and Trust in Collaborative Control,
European Control Conference 2009 – ECC‘09. 23-AUG-09, . : ,

09/25/2014 98.00 T. Jiang , P. Purkayastha, J. S. Baras. Constrained Coalitional Games and Networks of Autonomous Agents,
Third International Symposium on Communications, Control and Signal Processing. 12-MAR-08, . : ,

09/25/2014 99.00 J.S. Baras , P. Hovareshti. Efficient and Robust Communication Topologies for Distributed Decision Making in Networked Systems,
48th IEEE Conference on Decision and Control. 16-DEC-09, . : ,

09/25/2014 00.00 J.S. Baras , T. Jiang. Composite Trust in Networked Multi-Agent Systems,
2012 American Control Conference. 01-JUN-12, . : ,

09/25/2014 01.00 J.S. Baras. Dynamic Distributed Control over Semirings and Applications,
SIAM Conference on Control and Its Applications (CT09). 06-JUL-09, . : ,

09/25/2014 02.00 J.S. Baras. Efficient Connectivity Topologies for Networked Control Systems,
SIAM Conference on Control and Its Applications (CT09). 06-JUL-09, . : ,

09/25/2014 03.00 J.S. Baras, P. Hovareshti, S. Perumal. Dynamic Self-Organization and Clustering in Distributed Networked Systems for Improvement,
Forty-Seventh Annual Allerton Conference on Communication, Control, and Computing (Allerton Conference 2009). 30-SEP-09, . : ,

09/25/2014 04.00 J.S. Baras, V. Tabatabaee, K.S. Jain. Component Based Modeling for Cross-layer Analysis of 802.11 MAC and OLSR Routing Protocols in Ad-hoc Networks,
MILCOM 2009 " The Challenge of Convergence. 18-OCT-09, . : ,

09/25/2014 05.00 J.S. Shin , V.D. Gligor. A New Privacy Enhanced Matchmaking Protocol,
Network and Distributed Systems Security Symposium (NDSS). 01-FEB-08, . : ,

09/25/2014 06.00 Jason J. Haas , Yih-Chun Hu. Communication Requirements for Crash Avoidance,
Seventh ACM International Workshop on Vehicular Ad Hoc Networks (VANET 2010). 01-SEP-10, . : ,

09/25/2014 07.00 Jason J. Haas, Yih-Chun Hu, Nicola Laurenti. Low-Cost Mitigation of Privacy Loss due to Radiometric Identification,
Eighth ACM International Workshop on Vehicular Ad Hoc Networks (VANET 2011). 01-SEP-11, . : ,

09/25/2014 08.00 Jerry T. Chiang , Yih-Chun Hu. Dynamic Jamming Mitigation for Wireless Broadcast Networks,
Twenty-Seventh Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM 2008). 01-APR-08, . : ,

09/25/2014 09.00 Jerry T. Chiang , Yih-Chun Hu. Extended Abstract: Cross-Layer Jamming Detection in Wireless Broadcast Networks,
Thirteenth Annual International Conference on Mobile Computing and Networking (MobiCom 2007). 01-SEP-07, . : ,

09/25/2014 10.00 Dongho Kim, Yih-Chun Hu, Jerry T. Chiang. JIM-Beam: using Spatial Randomness to Build Jamming-Resilient Wireless Flooding Networks,
thirteenth ACM international symposium on Mobile Ad Hoc Networking and Computing (MobiHoc 2012). 01-JUN-12, . : ,

09/25/2014 11.00 Jihyuk Choi, Dongho Kim, Jerry T. Chiang, Yih-Chun Hu. . Partial Deafness: a Novel Denial-of-Service Attack in 802.11 Networks,
Sixth International ICST Conference on Security and Privacy in Communication Networks (SecureComm 2010). 01-SEP-10, . : ,

09/25/2014 12.00 Jihyuk Choi, Sang-Yoon Chang, Diko Ko, Yih-Chun Hu. Secure MAC-Layer Protocol for Captive Portals in Wireless Hotspots,
IEEE International Conference on Communications (ICC 2011). 01-JUN-11, . : ,

09/25/2014 13.00 Jonathan McCune, Yanlin Li, Stephen Zhou, Ning Qu, Anupam Datta, Virgil Gligor, Adrian Perrig. TrustVisor: Efficient TCB Reduction and Attestation,
IEEE Symposium on Security and Privacy. 01-MAY-10, . : ,

09/25/2014 14.00 Juan Garay, Jonathan Katz, Ranjit Kumaresan, Hong-Sheng Zhou. Adaptively Secure Broadcast, Revisited,
ACM Symposium on Principles of Distributed Computing (PODC). 01-JAN-11, . : ,

09/25/2014 15.00 Jure Leskovec, Andreas Krause, Carlos Guestrin, Christos Faloutsos, Jeanne VanBriesen , Natalie Glance. Cost-effective Outbreak Detection in Networks,
13th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (KDD). 01-AUG-07, . : ,

09/25/2014 16.00 K. K. Somasundaram, J.S. Baras. Semiring Pruning for Information Dissemination in Mobile Ad Hoc Networks,
First International Conference on Networks & Communications (NetCoM-2009). 27-DEC-09, . : ,

09/25/2014 17.00 K. Somasundaram, J.S. Baras. Evolutionary Dynamics of Collaborative Environments with Heterogeneous Agents,
17th Mediterranean Conference on Control and Automation (MED'09). 24-JUN-09, . : ,

09/25/2014 18.00 K. Somasundaram, J.S. Baras. Local Pruning for Information Dissemination for the Idempotent Semiring Algebraic Path Problem,
2010 International Symposium on Mathematical Theory of Networks and Systems. 05-JUL-10, . : ,

09/25/2014 19.00 J. S. Baras , K.K. Somasundaram . Achieving Symmetric Pareto Nash Equilibria using Biased Replicator Dynamics,
48th IEEE Conference on Decision and Control. 16-DEC-09, . : ,

09/25/2014 20.00 K.K. Somasundaram , J.S. Baras. Performance Improvements in Distributed Estimation and Fusion Induced by a Trusted Core,
Proceedings of the 12th International Conference on Information Fusion-Fusion 2009. 06-JUL-09, . : ,

09/25/2014 21.00 Khalid El-Arini, Gaurav Veda, Dafna Shahaf, Carlos Guestrin . Turning Down `the Noise in the Blogosphere,
Knowledge Discovery and Data Mining (KDD). 01-JUN-09, . : ,

09/25/2014 22.00 Kyoung-Dae Kim , P. R. Kumar. Architecture and Mechanism Design for Real-Time and Fault-Tolerant Etherware for Networked Control,
17th World Congress, The International Federation of Automatic Control. 06-JUL-08, . : ,

09/25/2014 23.00 Kyoung-Dae Kim , P. R. Kumar. Design and experimental verification of real-time mechanisms for middleware for networked control,
American Control Conference-ACC2010. 30-JUN-10, . : ,

09/25/2014 24.00 Kyoung-Dae Kim, Sayan Mitra, P. R. Kumar. Bounded ?-Reachability of Linear Hybrid Automata with a Deterministic and Transversal Discrete Transition Condition,
49th IEEE Conference on Decision and Control. 15-DEC-10, . : ,

09/25/2014 25.00 Kyoung-Dae Kim, Sayan Mitra , P. R. Kumar. Computing Bounded ?-Reach Set with Finite Precision Computations for a Class of Linear Hybrid Automata,
14th International Conference on Hybrid Systems: Computation and Control (HSCC 2011). 12-APR-11, . : ,

09/25/2014 26.00 L. Bui, R. Srikant, A. L. Stolyar. Novel Architectures and Algorithms for Delay Reduction in Back-pressure Scheduling and Routing,
INFOCOM Mini-Conference. 01-JAN-09, . : ,

09/25/2014 27.00 M. Leconte, J. Ni, R. Srikant, L. Jiang, J. Walrand. Fast Mixing of Parallel Glauber Dynamics and Low-Delay CSMA Scheduling,
IEEE INFOCOM Min-Conference. 01-JAN-11, . : ,

09/25/2014 28.00 M. Anand, P. R. Kumar. A digital interface for Gaussian relay networks: lifting codes from the discrete superposition model to Gaussian relay networks,
2010 IEEE Information Theory Workshop. 06-JAN-10, . : ,

09/25/2014 29.00 M. Conti, R. Poovendran, M. Seccheiro. FakeBook: Detecting Fake Profiles in On Line Social Networks,
," first International Workshop on Cyber Security of Online Social Network (CSOSN 2012). 25-AUG-12, . : ,

09/25/2014 30.00 M. Leconte, J. Ni, R. Srikant. Improved Bounds on the Throughput Efficiency of Greedy Maximal Scheduling in Wireless Networks,
ACM MobiHoc. 01-JAN-09, . : ,

09/25/2014 31.00 M. Raya, P. Papadimitratos, V.D. Gligor, J.-P. Hubaux. On Data-Centric Trust Establishment in Ephemeral Ad-Hoc Networks,
INFOCOM 2008. 01-APR-08, . : ,

09/25/2014 32.00 Martin Albrecht, Craig Gentry, Shai Halevi, . Attacking Cryptographic Schemes,
ACM Conference on Computer and Communications Security. 01-JAN-09, . : ,

09/25/2014 33.00 Maxwell Krohn, Phen-Lan Lin, Adrian Perrig, Hung-Min Sun, Bo-Yin Yang. SPATE: Small-group PKI-less Authenticated Trust Establishment,
ACM MobiSys. 01-JUN-09, . : ,

09/25/2014 34.00 Nitin Vaidya, Lewis Tseng, Guanfeng Liang. Iterative Approximate Byzantine Consensus in Arbitrary Directed Graphs,
ACM Symposium on Principles of Distributed Computing (PODC). 01-JUL-12, . : ,

09/25/2014 35.00 P. Hovareshti , J. S. Baras. Efficient Communication Infrastructures for Distributed Control and Decision Making in Networked Stochastic Systems,
19th International Symposium on Mathematical Theory of Networks and Systems (MTNS 2010). 05-JUL-10, . : ,

09/25/2014 36.00 P. Hovareshti, J. S. Baras , V. Gupta. Average Consensus over Small World Networks: A Probabilistic Framework,
47th IEEE Conference on Decision and Control. 09-DEC-08, . : ,

09/25/2014 37.00 P. L. Yu, J. S. Baras , B. M. Sadler. Multicarrier Authentication at the Physical Layer,
IEEE Workshop on Security and Privacy in Wireless Networks (IEEE SPAWN 2008). 23-JUN-08, . : ,

09/25/2014 38.00 P. L. Yu, J. S. Baras, B. M. Sadler. Power Allocation Tradeoffs in Multicarrier Authentication Systems,
26th Army Science Conference . 01-DEC-08, . : ,

09/25/2014 39.00 P. Purkayastha , J. S. Baras. Convergence Results for Ant Routing Algorithms via Stochastic Approximations,
13th International Conference on Hybrid Systems: Computation and Control (HSCC '10). 12-APR-10, . : ,

09/25/2014 40.00 P. Tague, D. Slater, J. Rogers , R. Poovendran. Vulnerability of Network Traffic under Node Capture Attacks using Circuit Theoretic Analysis,
INFOCOM. 01-JAN-08, . : ,

09/25/2014 41.00 P. Tague, M. Li , R. Poovendran. Probabilistic Mitigation of Control Channel Jamming via Random Key Distribution,
IEEE Annual International Symposium on Personal Indoor and Mobile Radio Communications (PIMRC). 01-JAN-07, . : ,

09/25/2014 42.00 J.S. Baras, B. M. Sadler, P. Yu. Physical Layer Authentication,
IEEE Transactions on Information Forensics and Security. 01-MAR-08, . : ,

09/25/2014 43.00 Parisa Haghani , Yih-Chun Hu. Power Control for Fair Dynamic Channel Reservation in VANETs,
9th IEEE Communications Society Conference (SECON 2012). 01-JUN-12, . : ,

09/25/2014 44.00 Patrick Tague, Sidharth Nabar, Jim Ritcey, David Slater , Radha Poovendran, . Throughput Optimization for Multipath Unicast Routing Under Probabilistic Jamming,
19th Annual IEEE International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC). 01-SEP-08, . : ,

09/25/2014 45.00 Q. Zhu, A. Clark, R. Poovendran , T. Basar. Deceptive Routing Games,
IEEE CDC 2012. 10-DEC-12, . : ,

09/25/2014 46.00 Qiao Li , Rohit Negi. Scheduling in Multi-hop Wireless Networks with Priorities,
IEEE Int. Conf. Infocom. 01-JAN-09, . : ,

09/25/2014 47.00 Qiao Li, Gyouhwan Kim, Rohit Negi. Maximal scheduling in a hypergraph model for wireless networks, IEEE Int. Conf. Communications. 01-MAY-08, . : ,

09/25/2014 48.00 Qing Li , Meiyuan Zhao , Jesse Walker, Yih-Chun Hu, Adrian Perrig, Wade Trappe. SEAR: A Secure Efficient Ad Hoc On Demand Routing Protocol for Wireless Networks,
3rd annual ACM Symposium on InformAtion, Computer and Communications Security (ASIACCS 2008). 01-MAR-08, . : ,

09/25/2014 49.00 Roberto Solis Robles, Jason J. Haas, Jerry T. Chiang, Yih-Chun Hu, P. R. Kumar. Secure Network-Wide Clock Synchronization in Wireless Sensor Networks,
49th IEEE Conference on Decision and Control. 15-DEC-10, . : ,

09/25/2014 50.00 Rosario Gennaro, Hugo Krawczyk, Tal Rabin . Secure Network Coding Over the Integers,
Public-Key Cryptography (PKC) . 01-JAN-10, . : ,

09/25/2014 51.00 S. Dov Gordon, Ranjit Kumaresan, Arkady Yerukhimovich . Authenticated Broadcast with a Partially Compromised Public-Key Infrastructure,
12th Intl. Symp. on Stabilization, Safety, and Security of Distributed Systems (SSS). 01-JAN-10, . : ,

09/25/2014 53.00 T. Ta, J.S. Baras, S. Jain. Wormhole Detection Using Channel Characteristics,
2012 IEEE International Conference on Communications (ICC'12), First International Workshop on Security and Forensics in Communication Systems (SFCS2012). 01-JUN-12, . : ,

09/25/2014 54.00 Sang-Yoon Chang, Yih-Chun Hu, Nicola Laurenti. Jamming-Resilient MAC-Layer Protocol for Wireless Channel Coordination,
Eighteenth Annual International Conference on Mobile Computing and Networking (MobiCom 2012). 01-AUG-12, . : ,

09/25/2014 52.00 S. Jain, J.S. Baras. Preventing Wormhole Attacks Using Physical layer Authentication,
2012 IEEE Wireless Communications and Networking Conference (WCNC2012). 01-APR-12, . : ,

09/25/2014 55.00 Sang-Yoon Chang, Yih-Chun Hu, Hans Anderson, Ting Fu, Evelyn Y. L. Huang. Body Area Network Security: Robust Key Establishment Using Human Body Channel,
3rd USENIX Workshop on Health Security and Privacy (HealthSec 2012). 01-AUG-12, . : ,

09/25/2014 56.00 T. Bonaci, L. Bushnell, R. Poovendran. Node capture attacks in wireless sensor networks: A system theoretic approach,
49th IEEE Control and Desicion Conference. 01-JAN-10, . : ,

09/25/2014 57.00 T. Ji, E. Athanasopoulou , R. Srikant. Counter-Examples to the Optimality of MWS-alpha Policies for Scheduling in Generalized Switches,
INFOCOM Mini-Conference. 01-JAN-09, . : ,

09/25/2014 58.00 T. Jiang, J.S. Baras. Coalition Formation Through Learning in Autonomic Networks,
International Conference on Game Theory and Networks (GameNets09). 13-MAY-09, . : ,

09/25/2014 59.00 T. Jiang, I. Matei, J. S. Baras. Trust Based Distributed Kalman Filtering Approach for Mode Estimation in Power Systems,
Proceedings of First Workshop on Secure Control Systems (SCS) as part of CPSWeek. 12-APR-10, . : ,

09/25/2014 60.00 T. Ta , J.S. Baras. Enhancing Privacy in LTE Paging System Using Physical Layer Identification,
17th European Symposium on Research in Computer Security (ESORICS 2012), 7th International Workshop on data Privacy Management (DPM). 10-SEP-12, . : ,

09/25/2014 61.00 Tamara Bonaci , Phillip Lee, Linda Bushnell, Radha Poovendran. Distributed Clone Detection in Wireless Sensor Networks: An Optimization Approach,
2nd IEEE International Workshop on Data Security and Privacy in Wireless Networks. 01-JUN-11, . : ,

09/25/2014 62.00 Tiffany Hyun-Jin Kim, Ahren Studer, Rituik Dubey, Xin Zhang, Adrian Perrig, Fan Bai, Bhargav Bellur, Aravind Iyer. VANET Alert Endorsement Using Multi-Source Filters,
ACM International Workshop on Vehicular Ad Hoc Networks (VANET). 01-SEP-10, . : ,

09/25/2014 63.00 V. Gligor, A. Perrig, J. Zhao. Brief encounters with a random key graph,
17th Security Protocols Workshop (SPW 17). 01-APR-09, . : ,

09/25/2014 64.00 V. I. Ivanov, P. L. Yu , J. S. Baras. Securing the Communication of Medical Information Using Local Biometric Authentication and Commercial Wireless Links,
International Symposium on Health Information Management Research (ISHIMR 2009). 14-OCT-09, . : ,

09/25/2014 65.00 Vinod Prabhakaran , P. R. Kumar. Communication by Sleeping: Optimizing a Relay Channel under Wake and Transmit Power Costs,
2009 IEEE International Symposium on Information Theory (ISIT 2009). 28-JUN-09, . : ,

09/25/2014 66.00 Virgil Gligor , Jeannette Wing. Towards a Theory of Trust in Networks of Humans and computers,
19th Security Protocols Workshop (SPW 17). 01-APR-11, . : ,

09/25/2014 67.00 W. Lin, Ming-Ting, Sun, R. Poovendran , Z. Zhan. Human Activity Recognition for Video Surveillance,
2008 IEEE International Symposium on Circuits and Systems (ISCAS). 18-MAY-08, . : ,

09/25/2014 68.00 W. Shi , J. Ritcey. Distributed jamming for secure communication in a Poisson field of legitimate nodes and eavesdroppers,,
Asilomar Conf. on Signals Systems Computers. 01-NOV-12, . : ,

09/25/2014 69.00 W. Shi , J. Ritcey. Performance of MMSE multi-antenna receiver under hierarchical Poisson random fields of interferences,
Asilomar Conf. on Signals Systems Computers. 01-NOV-12, . : ,

09/25/2014 70.00 W. Shi, JA Ritcey. Transmit beam forming and cooperative jamming for MIMOME wiretap channels,
Asilomar Conference on Signals, Systems, and Computers. 01-NOV-11, . : ,

09/25/2014 71.00 Weiyao Lin, Ming-Ting Sun, Radha , Zhengyou Zhang. Group Event Detection for Video Surveillance,
International Symposium on Circuits and Systems (ISCAS'09). 01-JAN-09, . : ,

09/25/2014 72.00 Xin Zhang , Adrian Perrig. Correlation-Resilient Path Selection in Multi-Path Routing,
IEEE Global Communications Conference (Globecom). 01-DEC-10, . : ,

09/25/2014 73.00 Xin Zhang, Abhishek Jain, Adrian Perrig. Packet-Dropping Adversary Identification for Data Plane Security,
ACM CoNext. 01-DEC-08, . : ,

09/25/2014 74.00 Xin Zhang, Adrian Perrig, Hui Zhang. Centaur: A Hybrid Approach for Reliable Policy-Based Routing,
the International Conference on Distributed Computing Systems (ICDCS). 01-JUN-09, . : ,

09/25/2014 75.00 Xin Zhang, Chang Lan, Adrian Perrig. Secure and Scalable Fault Localization under Dynamic Traffic Patterns,
IEEE Symposium on Security and Privacy. 01-MAY-12, . : ,

09/25/2014 76.00 Xin Zhang , Hsu-Chun Hsiao, Geoffrey Hasker, Haowen Chan, Adrian Perrig, David Andersen. SCION: Scalability, Control, and Isolation On Next-Generation Networks,
IEEE Symposium on Security and Privacy. 01-MAY-11, . : ,

09/25/2014 77.00 Xin Zhang, Zongwei Zhou, Geoff Hasker, Adrian Perrig, Virgil Gligor. Network Fault Localization with Small TCB,
IEEE International Conference on Network Protocols (ICNP). 01-OCT-11, . : ,

09/25/2014 78.00 Xin Zhang, Zongwei Zhou, Hsu-Chun Hsiao, Tiffany Hyun-jin Kim, Adrian Perrig , Patrick Tague. ShortMAC: Efficient Data-Plane Fault Localization,
Proceedings of Networked and Distributed System Security Symposium (NDSS). 01-FEB-12, . : ,

09/25/2014 79.00 Yan Gao, P. R. Kumar. Joint Congestion Control and Random Access MAC in Multi-hop Wireless Networks via a Simplified Model,
48th IEEE Conference on Decision and Control. 16-DEC-09, . : ,

09/25/2014 80.00 Yan Gao, Chee Wei Tan, Ying Huang, Zheng Zeng, P. R. Kumar. Feasibility and Optimization of Delay Guarantees for Non-homogeneous Flows in IEEE 802.11 WLANs,
30th IEEE International Conference on Computer Communications (IEEE INFOCOM 2011). 10-APR-11, . : ,

09/25/2014 81.00 Yan Gao, Zheng Zeng , P. R. Kumar. Joint Random Access and Power Selection for Maximal Throughput in Wireless Networks,
Infocom Miniconference 2010 . 15-MAR-10, . : ,

09/25/2014 82.00 Yue-Hsun Lin, Ahren Studer, Hsu-Chun Hsiao, Jonathan McCune, King-Hang Wang, Maxwell Krohn, Phen-Lan Lin, Adrian Perrig, Hung-Min Sun, Bo-Yin Yang. SPATE: Small-group PKI-less Authenticated Trust Establishment,
ACM MobiSys. 01-JUN-09, . : ,

09/25/2014 83.00 Zheng Zeng, Yan Gao, P. R. Kumar, Kun Tan. CHAIN: Introducing Minimum Controlled Coordination into Random Access MAC,
30th IEEE International Conference on Computer Communications (IEEE INFOCOM 2011). 10-APR-11, . : ,

TOTAL: 146

Number of Peer-Reviewed Conference Proceeding publications (other than abstracts):

(d) Manuscripts

Received Paper

TOTAL:

Number of Manuscripts:

Books

Received	Book
09/25/2014 84.00	G. Theodorakopoulos, J. S. Baras. Path Problems in Networks: Algebraic, Analytical and Computational Methods, University of Maryland: Morgan & Claypool Publishers, (01 2010)
09/25/2014 85.00	G. Theodorakopoulos, J.S. Baras . Path Problems in Networks, University of Maryland: Morgan & Claypool Publishers, (01 2010)
09/25/2014 86.00	Liang-Liang Xie , P. R. Kumar. Information-Theoretic Studies of Wireless Sensor Networks, University of Maryland: IEEE-Wiley, (01 2009)

TOTAL: **3**

Received	Book Chapter

TOTAL:

Patents Submitted

Please see Attachment

Patents Awarded

Awards

J.S. Baras, "COMPASS: Component-based Architectures for Systems Synthesis", invited keynote address, 2012 MODPROD conference, February 8, 2012, Linkoping, Sweden.

P. R. Kumar, ACM SIGMOBILE Outstanding Contribution Award, 2012. For "pioneering contributions to the foundations of asymptotic performance analysis of large scale wireless networks."

P. R. Kumar, Distinguished Alumnus Award, IIT Madras, 2012.

R. Srikant , Distinguished Lecturer, IEEE Communications Society, 2012-2013
WiOpt 2012 Best Paper Award, http://wi-opt.cs.upb.de/WiOpt_2012/Home.html

V. Gligor, IEEE Computer Society Technical Achievement Award, June 2013

Graduate Students

NAME	PERCENT_SUPPORTED	Discipline
Please see attachement	0.00	
FTE Equivalent:	**0.00**	
Total Number:	**1**	

Names of Post Doctorates

NAME	PERCENT_SUPPORTED
Please see attachement	0.00
FTE Equivalent:	**0.00**
Total Number:	**1**

Names of Faculty Supported

NAME	PERCENT_SUPPORTED	National Academy Member
Please see attachement	0.00	
FTE Equivalent:	**0.00**	
Total Number:	**1**	

Names of Under Graduate students supported

NAME	PERCENT_SUPPORTED	Discipline
Please see Attachement	0.00	
FTE Equivalent:	**0.00**	
Total Number:	**1**	

Student Metrics

This section only applies to graduating undergraduates supported by this agreement in this reporting period

The number of undergraduates funded by this agreement who graduated during this period: 0.00

The number of undergraduates funded by this agreement who graduated during this period with a degree in science, mathematics, engineering, or technology fields:..... 0.00

The number of undergraduates funded by your agreement who graduated during this period and will continue to pursue a graduate or Ph.D. degree in science, mathematics, engineering, or technology fields:..... 0.00

Number of graduating undergraduates who achieved a 3.5 GPA to 4.0 (4.0 max scale):..... 0.00

Number of graduating undergraduates funded by a DoD funded Center of Excellence grant for Education, Research and Engineering:..... 0.00

The number of undergraduates funded by your agreement who graduated during this period and intend to work for the Department of Defense 0.00

The number of undergraduates funded by your agreement who graduated during this period and will receive scholarships or fellowships for further studies in science, mathematics, engineering or technology fields: 0.00

Names of Personnel receiving masters degrees

NAME
Please see attachment
Total Number: 1

Names of personnel receiving PHDs

NAME
Please see attachement
Total Number: 1

Names of other research staff

NAME	PERCENT_SUPPORTED
none	0.00
FTE Equivalent:	**0.00**
Total Number:	**1**

Sub Contractors (DD882)

Inventions (DD882)

Scientific Progress

(4) Scientific progress and accomplishments (Description should include significant theoretical or experimental advances)

Our research is in the area of design and operation of reliable and secure tactical MANET. The emphasis of our research was on the discovery and development of methods and algorithms that can unify the investigation of resiliency and security for MANETs. With this emphasis, we investigated fundamental problems addressing the characterization, properties and design of the Trusted Core of a MANET. More specifically we investigated several research problems in the context of Tasks 1 – 4 (Thrusts 1-4).

(4.1) Thrust 1: Design of Dependable Trusted Core of MANET

Several efforts were made to realize the vision of the trusted core sub-network. More specifically, our focus was on Message and Device Authentication in MANETs. In this area, we pursued the following specific topics:

(4.1.1) Message, Node, and Device Authentication in MANETs

(1) Authentication of Fingerprint Scanners

To counter certain security threats in biometric authentication systems, particularly in portable devices (e.g., phones and laptops), we have developed a technology for automated authentication of fingerprint scanners of exactly the same type, manufacturer, and model. The technology uses unique, persistent, and unalterable characteristics of the fingerprint scanners to detect attacks on the scanners, such as detecting an image containing the fingerprint pattern of the legitimate user and acquired with the authentic fingerprint scanner replaced by another image that still contains the fingerprint pattern of the legitimate user but has been acquired with another, unauthentic fingerprint scanner. The technology uses the conventional authentication steps of enrolment and verification, each of which can be implemented in a portable device, a desktop, or a remote server. The technology is extremely accurate, computationally efficient, robust in a wide range of conditions, does not require any hardware modifications, and can be added (as a software add-on) to systems already manufactured and placed into service. We have also implemented the technology in a demonstration prototype for both area and swipe scanners. Further, we have demonstrated how this physical layer technique can be combined with other physical layer techniques like TPM, MTM, TCN and modulation watermarking tags to strengthen considerably the security of mobile wireless devices and networks.

(4.1.2) Securing Neighborhood Discovery in MANETs using Physical Layer Authentication

Mobile ad-hoc networks (MANETs) are a key enabler of pervasive computing. Constrained resources in mobile stations make it critical for nodes to be able to cooperate to enhance communication and computation capabilities. However, the wireless and dynamic nature of the links presents easy attack vectors for adversaries. The ability to securely discover and identify neighboring nodes (secure ND) is a fundamental building block for such networks. Even a relatively weak adversarial relay has the capability of distorting the network view and diverting significant amount of traffic. This can cause significant performance degradation. In our work, we utilized a physical layer authentication scheme to secure neighborhood discovery against adversarial relays. Our proposed method incurs little performance overhead and requires no additional hardware. We developed analytical and performed simulation based performance evaluations of the security of our scheme. We also demonstrated that the scheme can be used efficiently to prevent wormhole attacks.

(4.1.3) Round-efficient broadcast authentication and signatures in general and specialized network topologies

We studied mechanisms for round-efficient broadcast authentication protocols for fixed topology classes. Although numerous efficient broadcast authentication techniques exist, we have identified significant improvements for authentication latency for existing protocols in specific communication topologies. Moreover, we have proposed new approaches for broadcast authentication. These are exciting results, because broadcast authentication has been studied for two decades. Our new results demonstrate lower bounds for broadcast authentication in various topologies, as well as protocols that match or get very close to these bounds.

More specifically, we consider resource-constrained broadcast authentication for n receivers in a static, known network topology. There are only two known broadcast authentication protocols that do not use asymmetric cryptography, one-time signatures, multi-receiver MACs, or time synchronization: the Guy Fawkes protocol by Anderson et al., and a protocol based on secure aggregation by Chan and Perrig. Both these protocols require three passes of a message front traversing the network. We investigate whether this amount of interaction can be improved efficiently for specific common topology classes, namely, linear topologies, tree topologies and fully connected topologies. We show modifications to the protocols allowing them to complete in just two passes in the linear and fully connected cases with a small constant factor increase in per-node communication overhead, and a further optimization that achieves the equivalent of just a single pass in the linear case with O (log(n)) increase in per-node communication overhead. We also prove new lower bounds for round complexity, or the maximum number of consecutive interactions in a protocol. We show that protocols with efficient per-node communication overhead (polylogarithmic in n) must require at least 2*log(n) rounds in any topology; this implies that our two-pass protocol in the fully-connected topology requires the fewest possible passes, and this bound is asymptotically tight for the full-duplex communication model. Furthermore, we show that communication-efficient protocols must take asymptotically more than 2*log

(n) rounds on trees; this implies that that there are some tree topologies for which two passes do not suffice and the existing three-pass algorithms may be optimal.

These new results will likely have a significant impact on the design of secure network protocols. For example in the case of secure routing protocols, our approach for broadcast authentication in linear topologies can enable efficient authentication along a network path. We will investigate the application of these protocols in the context of our project.

(4.2) Thrust 2: Adaptive Protocol Monitoring for Efficiency and Dependability

(4.2.1) Routing Protocol Monitoring for Wormhole Detection

The potential applications and pervasive nature of mobile ad-hoc networks (MANETs) has made them an attractive target for attackers. The wireless medium of communication coupled with constrained resources enable attacks, which can be executed by a weak adversary. A wormhole is one such attack, which poses considerable threat, particularly to routing protocols. In this attack, two adversarial nodes create a low latency out-of-band link (wormhole), either via external hardware or tunneling through network nodes. The attackers thus provide a path with low hop count. Typical MANET routing algorithms, such as AODV and DSR, select such links for routing, allowing the adversary to draw large amounts of network traffic. Such high traffic links under adversarial control can cause significant leakage of network secrets, performance degradation and congestion in the network. In our work, we devised a novel scheme for detecting a wormhole by utilizing the inherent symmetry of electromagnetic wave propagation in the wireless medium. We demonstrated the loss of this symmetry in the case of a wormhole attack and proposed a method to detect and flag the adversary. We modified the insecure neighborhood discovery to incorporate authentication. We further extended this scheme to a trust system with low overhead.

Our scheme operates independent of the higher layer MAC and routing protocols. We assume the existence of some form of contention management scheme for access to the wireless channel. For authentication during the neighborhood discovery phase, the scheme will perform well with any MAC and higher layer protocol. However, to build trust systems, we require the packet reception to be acknowledged. Thus, any MAC protocol that ensures instant feedback after packet reception will suffice, for example, the 802.11 MAC. We assumed the adversarial behavior to be limited to relaying and any offline attacks. In case of a relay with the capability to modify the packets, we can couple our scheme with any higher layer protocol used to ensure integrity of the messages in the network. For example, any form of a message authentication code will serve this purpose. It should be noted that hidden wormholes typically cannot be thwarted by higher layer cryptographic schemes. The benefits of our scheme thus complement the higher layer cryptographic methods.

(4.2.2) Trusted Multi-Agent Cores in Distributed Inference and Control

We investigated fundamental problems of modeling and representation of distributed multi-agent inference and decision making problems and we developed a new general model for such systems that involves constrained coalitional games and several interacting dynamic multigraphs, with nodes and links annotated by weights (including vector and logical ones). The framework emphasizes observables, partial information and de-emphasizes state models. The approach is justified on foundational principles. We then proceeded to develop a detailed model that involves models of the collaboration and communication multi-graphs between the agents. We developed new optimization-based analytics and new stochastic models for these problems that allow a careful analysis of the impact of the communication topology on performance. We also investigated extensions to algebraic structures involving partially ordered semirings, which allow the incorporation of logic-based strategies. We further extended the framework to allow the incorporation of adversaries including collaborating ones.
To provide a more fundamental understanding on how to model and analyze multi-agent systems in the presence of adversaries, we investigated distributed inference and learning problems in networked systems with adversaries. We analyzed the effects of adversarial attacks on the solutions and characterized the solution robustness and resiliency as functions of network topology and adversary distribution. We demonstrated that the existence of a small “trusted core” that provides substantial improvements to solution robustness and resilience. We characterized these improvements as functions of the degree of trust, connectivity and location of trusted nodes. We introduced value-directed graphs with weighted nodes as our model for composite trust, and included not only numerical weights, but also constraints. We showed that the semiring-based constraint satisfaction problem (SCSPs) framework can serve as the unified model to investigate trust relation establishment and its effect on performance of trusted cores of multiple agents.

As an application of these fundamental concepts and constructs we considered ad hoc networks, which rely on the mutual cooperation among individual nodes to achieve network-wide objectives. However, individual nodes may behave selfishly in order to maximize their own benefits without considering the global benefits of the network. One approach to incentivize nodes cooperation for better global benefits is to establish trust relations among nodes to guide their decision making. In our research work during this period, we developed a game theoretic analysis for the efficiency of establishing trust for improving node cooperation. The trust relations among nodes are modeled as a trust-weighted network, and we studied a graphical game in this network where the nodes’ payoffs are affected by their trust relations. We characterized the Nash equilibrium and the social optimum of this game and showed that the game efficiency has a close relationship to the Bonacich centralities of nodes in the trust-weighted network. Furthermore, we proposed an improvement of game efficiency by introducing heterogeneous resources

to nodes according to their centralities. We provided both experimental and theoretical analysis on the improvement of the game efficiency.

(4.3) Thrust 3: Network Utility Maximization

(4.3.1) An Axiomatic Clean Slate Approach To Secure Wireless Networking

Traditionally, wireless network protocols have been developed for performance. Subsequently, as attacks are identified, patches or defenses are developed. This leads to an “arms race,” where one is never confident about what other vulnerabilities may be exposed in the future. We seek to reverse this process. We identify a set of axioms, under which we develop an optimally secure utility maximized network. Our results rest on the axioms, and can be attacked only to the extent that the axioms can be challenged. We present a complete suite of protocols, taking a wireless network all the way from startup to optimality. These protocols are not just individually secure, they are holistically secure, that is, there are no gaps between them that can be attacked.

Consider a group of wireless nodes some of which are good, and the rest, bad. The good nodes seek to form a functioning wireless network, operating at some measure of utility. The bad nodes know the identities of the good nodes but not conversely. Moreover, unlike their good counterparts, the bad nodes are capable of fully centralized cooperation and collusion. On the other hand, the good nodes arrive on the scene unsynchronized, uncoordinated and ignorant of the others' intentions.

We introduce a distributed protocol that enables the good nodes to proceed all the way from primordial birth to a Min-Max utility optimal network, where the minimization is over all bad behaviors of the bad nodes, and the maximization is over all protocols followed by the good nodes. That is, the good nodes form a functioning, reliable network from startup, in the face of any sustained cooperative attack mounted by the bad nodes. We show that the protocol overhead occupies an arbitrarily small fraction of the total operating lifetime. We prove that no other protocol can attain a higher level of utility.

Our protocol supersedes a considerable amount of previous work that deals with several classes of attacks such as the following: man-in-the middle, wormholes, dropping packets, Byzantine behaviors, disruption of timing events, presenting false topologies, etc. More importantly, this protocol obviates the need to identify all of the other types attacks that can potentially be carried out by colluding malicious nodes, for there are many. Instead, this protocol forces the malicious nodes to just one of two behaviors: comply with the protocol as a proper participant, or jam from the outside.

(4.3.2) Multi-criteria Optimization, Resilience, and Robustness

Network utility maximization suggests a decomposition by which congestion, routing, MAC and other layers of the network protocol stack naturally arise from duality theory. In this project, our goal has been to study the resilience and robustness of the MAC protocols. In particular, we have been interested in the resilience and robustness of the protocol to the following factors:
(i) Limited communication and computational capability of the nodes
(ii) Imperfect carrier sensing
(iii) Impact of dynamics in the network topology
(iv) Impact of dynamics in the flow composition in the network.
The main feature of the protocol developed by us is the use of queue length information in assigning weights to links in the network. This assignment of weights also allows us to easily incorporate trust metrics developed in other parts of this MURI project in our MAC protocol. For example, our protocol continues to perform well if the link weights are multiplied by a constant. Thus, if a trust metric is available, we could multiply the link to boost or inhibit the use of a link by the MAC protocol. We now summarize our accomplishments in each of the four categories above.

(i) It had been shown by others that CSMA-type random access algorithms can achieve the maximum possible throughput in ad hoc wireless networks. However, these algorithms assume an idealized continuous-time CSMA protocol where collisions can never occur. In addition, simulation results indicate that the delay performance of these algorithms can be quite bad. On the other hand, although some simple heuristics (such as distributed approximations of greedy maximal scheduling) can yield much better delay performance for a large set of arrival rates, they may only achieve a fraction of the capacity region in general. In this project, we proposed a discrete-time version of the CSMA algorithm. Central to our results is a discrete-time distributed randomized algorithm which is based on a generalization of the so-called Glauber dynamics from statistical physics, where multiple links are allowed to update their states in a single time slot. The algorithm generates collision-free transmission schedules while explicitly taking collisions into account during the control phase of the protocol, thus partially relaxing the perfect CSMA assumption. More importantly, the algorithm allows us to incorporate mechanisms which lead to very good delay performance while retaining the throughput-optimality property.

(ii) In (i) above throughput-optimality is established under the assumption that each link can precisely sense the presence of other active links in its neighborhood. Going further, we investigated the achievable throughput of the CSMA algorithm under imperfect carrier sensing. Through the analysis on both false positive and negative carrier sensing failures, we show that CSMA

can achieve an arbitrary fraction of the capacity region if certain access probabilities are set appropriately. To establish this result, we use the perturbation theory of Markov chains.

(iii) In (i) and (ii) above, each link of the wireless network has two parameters: a transmission probability and an access probability. The transmission probability of each link is chosen as an appropriate function of its queue length, however, the access probabilities are simply regarded as some random numbers since they do not play any role in establishing the network stability, other than in dealing with imperfect carrier sensing. In this paper, we show that the access probabilities control the mixing time of the CSMA Markov chain and, as a result, affect the delay performance
of the CSMA. In particular, we derive formulas that relate the mixing time to access probabilities and use these to develop the following guideline for choosing access probabilities: for each link I should choose I set its access probability equal to 1/(d+1), where d is the number of links which interfere with link i. Simulation results show that this choice of access probabilities results in good delay performance.

(iv) We have primarily focused on the resilience and robustness of the MAC protocol to the dynamics of flow composition in the network. It is by now well-known that wireless networks with ¿le arrivals and departures are stable if one uses a class of congestion control mechanisms called alpha-fair congestion control mechanisms, and back-pressure based scheduling and routing. In recent work, we have shown that stability can be ensured even with very simple congestion control mechanisms, such as a ¿xed window size scheme, which limits the maximum number of packets that are allowed into the ingress queue of a ¿ow. A key ingredient of our result is the use of the difference between the logarithms of queue lengths as the link weights. This is exactly the weight function used in our MAC protocol. The results suggests that the MAC protocol alone leads to considerable resiliency in the network protocol stack, and stability is maintained even if different flows in the network use different transport-layer protocols, and even if the flows in the network dynamically change with time.

(4.3.3) Multi-metric Shortest Path Algorithms for Secure Routing

We completed the investigation of partially ordered semiring frameworks for robust pruning in MANET routing and hierarchical routing as well as multi-metric problems in multi-scale networks and analyzed connections to the Algebraic Stochastic Shortest Path Problem which led to new solutions and algorithms for pruning and topology dissemination for MANET. We introduced and investigated the stable path topology control problem for link-state routing in mobile multihop networks. We adopted a graph pruning approach to reduce the broadcast storm problem for link state routing: by selecting a subset of the graph topology to be broadcast, the broadcast storm can be reduced. Several of the pruning mechanisms proposed in the literature are distributed localized algorithms. One important metric for routing in wireless multi-hop networks is path stability. Although path stability has been studied for many reactive distance vector schemes, there is little work that addresses topology control for stable paths in link state routing. We introduced a new topology control algorithm that guarantees stable path routing: a mechanism that prunes the initial topology (to reduce the broadcast storm) while guaranteeing that the stable paths (for unicast routing) from every host to any target station are preserved in the pruned topology. We developed a multi-agent optimization framework where the decision policies of each agent are restricted to local policies on incident edges and independent of the policies of other agents. We showed that under a condition called the positivity condition, these independent local policies preserve the stable routing paths globally. We also provided an efficient and distributed algorithm, which we call the Stable Path Topology Control Algorithm, to compute this local policy that yields a pruned graph. We applied these analytic methods to develop provably secure MANET routing protocols, where the two metrics (e.g. link metrics) for example can be for example path delay and path trust.

(4.3.4) Selfish Misbehavior in Scheduling Algorithms of Wireless Networks:

We consider the problem of selfish misbehavior in scheduling algorithms of wireless networks. The wireless medium is a shared medium and simultaneous data transmission over conflicting links is not desirable. A scheduling algorithm determines the set of links to be activated at any given time such that the interference constraints of the wireless network are not violated. Scheduling algorithms are often designed under the assumption that network users will follow the algorithm specifications properly. We considered two scenarios in which a selfish user misbehaves from the protocol in order to achieve better performance such as higher throughput or less delay. The primary goal of a selfish user is to improve its own performance, but its greedy misbehavior usually results in performance degradation of honest hosts. In particular, we consider selfish misbehavior in cross-layered rate control algorithm of wireless networks. A cross-layered approach to rate control is a mechanism in which the network jointly optimizes data rates of the users and link schedules. Cross-layered rate control algorithm of wireless networks is equivalent to a utility optimization framework, which can be decomposed into two components: rate control at the transport layer and scheduling at the MAC layer. We present a scenario in which a selfish user misbehaves in order to obtain higher throughput. We consider a wireless network in which the link capacities change over time and users of the network are involved in the process of measuring and estimating the link capacities. A selfish user may misbehave in this process and mislead the scheduler about the actual value of its link capacity. We find an equivalent optimization framework that captures misbehavior pattern of the selfish user. We impose a cost term on the utility function of the users in order to prevent such a selfish misbehavior. Penalties and rewards provide strong mechanisms for solving network problems and achieving performance objectives. We find the cost term in a network in which the conflict graph is a complete graph. In this case, at each time instance, at most one link can be activated for data transmission. We determined, for this network, which cost function prevents

selfish misbehavior. We also developed a heuristic for identifying a cost function in an arbitrary network.

(4.4) Thrust 4: Threat Modeling Detection and Defense in MANETs

(4.4.1) Detection of Adversary-Induced Faults

In MANETs, which are multi-hop wireless networks, the path between a source and a destination may often contain multiple hops, and data packets are relayed on the different hops from the source to the destination. This multi-hop nature makes the wireless networks subject to adversary-induced faults and tampering attacks; e.g., a compromised or misbehaving node can tamper packets it forwards. We have investigated mechanisms for the detection of such tampering attack in wireless networks.

(1) Watchdogs with Source Coding:
The well-known watchdog mechanism is a monitoring method used for ad hoc networks, and is the basis of many misbehavior detection algorithms, and trust or reputation systems. The basic idea of the watchdog mechanism is that the network nodes (acting as watchdogs) police their downstream neighbors locally, using overheard messages, in order to detect misbehavior. If a watchdog detects that a packet is not forwarded within a certain period, or is altered by its neighbor before forwarding, it deems the neighbor as misbehaving. When the misbehavior rate for a node surpasses certain threshold, the source is notified and subsequent packets are forwarded along routes that exclude the misbehaving node. The main challenge for the watchdog mechanism is the unreliable wireless environment. Due to channel fading and interference, even when the transmitter and the watchdog are both within communication range, the watchdog may not be able to overhear every transmission, and therefore may be unable to determine whether packets were tampered. So it is possible that the watchdogs will not detect an attacker.

To mitigate the misbehavior of the malicious nodes, a watchdog mechanism must achieve the following two goals: malicious behavior in the network should be detected with high probability, and, in the absence of an attack, the throughput under the detection mechanism should be comparable to the throughput without detection. These two goals seem to be conflicting. On the one hand, more redundancy is required to improve the probability of detection. On the other hand, higher throughput requires redundancy to be reduced. However, we have showed that both goals can be achieved simultaneously by introducing error detection coding to the watchdog mechanism. We have developed a computationally simple scheme that integrates source error detection coding and the watchdog mechanism. We showed that by choosing the coding scheme properly, a misbehaving node would be detected with high probability, without degrading the throughput much, even if the watchdog can only overhear a fraction of the packets. We also developed a protocol that identifies the misbehaving node using two watchdog nodes per potentially misbehaving relay node. We also showed that, together with source error detection coding, the probability of correctly locating the malicious node can be made close to one.

We further extended this work to explore the impact of packet tampering, and the use of watchdogs, on TCP flows. In particular, we observed the phenomenon of watchdog-induced packet losses with TCP flows. Such losses can occur even in the absence of packet tampering by an attacker, when the notifications from the watchdog are delayed. The TCP receiver, due to such a delayed notification, will not be able to send a TCP ACK, potentially causing the TCP sender to timeout. Such a timeout causes the TCP sender to behave as if a packet is lost along the route, and it responds by performing congestion control, degrading TCP throughput. We have developed simple mechanisms to reduce the impact of such watchdog-induced packet losses, and evaluated the ability of our mechanisms to improve performance.

The watchdog mechanism can also be applied in the case when the MANET uses multiple channels. With the use of multiple channels, it is beneficial for the different nodes to transmit on different channels, to improve performance. However, such a channel usage can also reduce the opportunities for the nodes to watch each other's transmissions to detect misbehavior. We identified this trade-off, and developed a strategy that can yield the performance benefits of multiple channels, while also attempting to ensure that watchdogs can observe forwarded packets for detection of misbehavior.

(2) Secure Capacity of Information Networks Without Monitoring
We have also investigated the secure capacity of information networks under tampering attacks. In particular, we studied the maximum achievable rate for a source-destination pair such that any attack by a compromised node can be detected. Significant research effort has been previously directed towards analysis of capacity with linear network coding. It has been shown by others that the error detection capacity with linear network coding is C-Z where C is the minimum cut between the source and the destination and Z is the mincut between the adversary and the destination. However, the adversary model assumed by this past work is a link-level model in which the adversary can attack any Z links in the network. In reality, the adversary is often node-level in the sense that the adversary captures a node and can attack all the out-going links from that node. We first characterized the secure capacity with end-to-end error detection, assuming that no intermediate nodes in the network monitor their neighbors (that is, no watchdogs). We restrict ourselves to the case when coding is only performed by the source, or by the neighbors of the source, and the remaining nodes optionally duplicate and forward the packets they receive. The problem of characterizing the achievable rates can then be formulated as an optimization problem. The solution of the optimization problem not only yields the maximum achievable rate, but also a routing strategy to achieve this rate. We also investigated the secure capacity with monitoring in which intermediate nodes can watch or monitor their neighbors and compare the packets they overhear. We showed that there exist networks in which secure capacity with such monitoring can be

arbitrarily larger than that without monitoring.

We also considered an approach wherein a traffic flow is carried on multiple node-disjoint routes, allowing different packets from the same flow to travel different subsets of such routes. Specifically, we considered the case where the flow may use any two of three disjoint routes for each packet on the flow. The goal now is to determine the best set of routes to be used for each packet, and the scheduling policy that can optimize the rates of the various flows. We achieved this goal by maintaining multiple virtual queues for each flow: one queue is for data that has not yet been sent to any receiver, and the other three queues are for data that has been sent on one of the disjoint paths. Virtual links with appropriate rates are added between the various queues, so as to capture the replication requirement correctly. We then use the utility optimization framework to develop a congestion control algorithm and a backpressure-based scheduler that can optimize the network utility under the disjoint route requirement. This approach can be generalized to more complex networks.

(4.4.2) Network Localization of Adversary Induced Faults

In our previous work, we showed that the ability of the trusted core (TC) to maintain effective communication despite link uncertainty (e.g., channel fading, interferences, environment obstacles, fluctuating weather patters), changing network topology and dynamic node membership, suggests two complementary approaches to adaptive communication protocol design: (1) stochastic network modeling and (2) machine learning. A central goal of our project is to achieve highly available network communication in the presence of active adversaries. In particular, we would like to provide lower bounds for network availability, such that the network can guarantee to provide useful throughput even in the presence of adversaries. We have considered several approaches to achieve these properties, and during the project we have designed two schemes, one based on cryptographic approaches and the other based on trusted hardware. Leveraging efficient fault localization, we can devise a network architecture that provides guaranteed throughput, based on the observation that attackers face a dilemma: if they misbehave and cause damage beyond a certain threshold, the fault localization will detect them and they will be removed; but if they cause less damage than the threshold, then they provide a useful level of bandwidth. Consequently, the network will provide a guaranteed level of throughput despite the adversaries.

We have three major accomplishments in the localization of adversary-induced faults: ShortMAC, DynaFL, and Assayer.

(1) ShortMAC
Previous fault localization protocols could not achieve a practical tradeoff between security and efficiency and they require unacceptably long detection delays, and require monitored flows to be impractically long-lived. We designed an efficient fault localization protocol called ShortMAC, which leverages probabilistic packet authentication and achieves 100-10000 times lower detection delay and overhead than related work. We theoretically derive a lower-bound guarantee on data-plane packet delivery in ShortMAC, implement a ShortMAC prototype, and evaluate its effectiveness using the SSFNet simulator and Linux/Click routers. Our implementation and evaluation results show that ShortMAC causes negligible throughput and latency costs while retaining a high level of security.

(2) DynaFL
Compromised and misconfigured routers are a well-known problem in ISP and enterprise networks. Data-plane fault localization aims to identify faulty links of compromised and misconfigured routers during packet forwarding, and is recognized as an effective means of achieving high network availability. Existing secure fault localization protocols are path-based, which assume that the source node knows the entire outgoing path that delivers the source node's packets and that the path is static and long-lived. However, these assumptions are incompatible with the dynamic traffic patterns and agile load balancing commonly seen in modern networks. To cope with real-world routing dynamics, we propose the first secure neighborhood-based fault localization protocol, DynaFL, with no requirements on path durability or the source node knowing the outgoing paths. Through delayed key disclosure, DynaFL incurs little communication overhead and a small, constant router state independent of the network size or the number of flows traversing a router. In addition, each DynaFL router maintains only a single secret key, which based on our measurement results represents 2-4 orders of magnitude reduction over previous path-based fault localization protocols.

(3) Assayer
As hardware support for improved end-host security becomes ubiquitous, it is important to consider how network security and performance can benefit from these improvements. If portions of each end-host can be trusted, then network infrastructure no longer needs to arduously and imprecisely reconstruct data already known by the end-hosts. Through the design of a general-purpose architecture we call Assayer, we explore issues in providing trusted host-based data, including the balance between useful data and user privacy, and the tradeoffs between security and efficiency. We also evaluate the usefulness of such information in several case studies. We implement and evaluate a basic Assayer prototype. Our prototype requires fewer than 1,000 lines of code on the end-host. End-hosts can annotate their outbound traffic in a few microseconds, and these annotations can be checked efficiently; even packet-level annotations on a gigabit link can be checked with a loss in throughput of only 13.1%.

(4.4.3) Consensus and Approximate Agreements in the Presence of the Adversary

(1) Reaching Approximate Consensus

In the MANETs, and in other networks as well, the different nodes in the network may need to agree on a consensus on a real-valued quantity as a function of values sensed or proposed by the different nodes in the network. For instance, clock synchronization is an example of this problem, wherein each node in the network proposes a value for the current time, and then the nodes must agree on a common notion of the current time as a function of the proposed values. Similarly, each node in the network may sense external parameters such as the temperature, and the nodes need to collaboratively agree on a common notion of the external temperature. We consider this problem in a setting wherein an adversary may have compromised some of the nodes in the network. The compromised nodes can attempt to cause the state of the good nodes to diverge. To tolerate such a threat, we have developed an iterative algorithm that can allow the good nodes to reach consensus on real-values parameters despite the presence of a bounded number of adversarial nodes. We have also characterized properties of the underlying directed graph topology that are necessary to be able to tolerate a specified number of compromised nodes. The iterative algorithm only requires local communication between each node and its neighbors, and allows directed or asymmetric links, which can occur in wireless networks due to asymmetries in interference or channel characteristics. The iterative algorithm uses very simple iterative computational steps to achieve its objective. We prove that when the underlying network graph satisfies certain graph-theoretic sufficient properties, the algorithm will achieve convergence to a valid value, in the convex hull of inputs at the good nodes, despite misbehavior by compromised nodes, when the number of such nodes does not exceed a specified threshold.

In wireless networks, due to transmission errors, the links have a lossy behavior. We have explored the impact of such lossy links on the performance of iterative consensus algorithms that utilize local communication and iterative computation. To make our treatment concrete, we considered the problem of computing the average of real-valued input at the nodes in the network. For instance, the real-valued input may be the value of the local clock at each node in the MANET, or data sensed by a local sensor. With these inputs, the nodes need to agree on the average value of the inputs at all the nodes in the network. When transmission losses occur, the traditional iterative algorithms for average consensus fail to reach convergence on the average value. Due to the message losses, the algorithms may often underestimate the average. We developed a novel mechanism to mitigate this shortcoming, by introducing a small amount of additional state at each node. The additional state, in effect, emulates a virtual buffer that holds information, which may otherwise be lost when messages are lost on wireless links. It has been proven that the proposed algorithm can converge to the average despite lossy behavior of the wireless links. The proposed algorithm provides useful insights on how to design iterative algorithms over wireless links.

(2) Improving Throughput of Agreements

The Byzantine model has been used to characterize arbitrary behaviors of an adversary. Thus, the model is useful when an adversary compromises nodes in the network. There has been significant research on agreement in presence of Byzantine nodes. Traditionally, the research on Byzantine agreement focuses on the total message or bit-complexity of achieving an agreement. In our work, we designed algorithms that can achieve optimal throughput of agreement, given the rate region of the underlying network. The throughput of agreement is defined as the long-term average of the number of information bits being agreed upon per unit time. We considered the problem under the constraint that each link in the system has a fixed finite capacity. This contribution is of interest in MANETs wherein a certain capacity on each link is allocated for the purpose of executing the agreement mechanisms. We identified necessary conditions for agreement throughput at rate R bits/unit time to be achievable in general networks. These necessary conditions serve as an upper bound on the agreement capacity. However, whether this bound is tight or not remains an open problem in general. We have developed an algorithm structure that is inspired by the literature on network coding. Following this structure, we designed capacity-achieving algorithms for four-node networks with at most one compromised node and arbitrary link capacity distribution, and also for a class of symmetric networks in which all links have the same capacity. While characterizing the exact Byzantine agreement capacity in general network topologies is still an open problem, we have also developed algorithms that are guaranteed to achieve a constant fraction of the capacity in arbitrary topologies.

We also investigated the communication complexity of agreement. The communication complexity of an algorithm C(L) is defined as the maximum of the total number of bits transmitted by all the nodes according to the algorithm until agreement on L bits is reached correctly, considering all possible misbehaviors of the faulty nodes. This measure of complexity is widely used by the distributed computing community. The per-bit communication complexity of an algorithm is then defined as C(L)/L. We have proposed a deterministic multi-valued algorithm that solves the Byzantine broadcast problem deterministically for L bits in a network with n nodes and at most $t<n/3$ faulty nodes, with C(L) approximately equal to $n(n-1)L/(n-t)$ bits for large L. Hence, for large L, this algorithm achieves per-bit complexity approaching $n(n-1)/(n-t)$, which is linear in n for non-trivial values of t. We are also able to prove that the per-bit complexity of the proposed algorithm is within a constant factor of 2 of optimal. Using ideas introduced in the deterministic multi-valued one-to-many Byzantine broadcast algorithm, we also designed a deterministic multi-valued all-to-all Byzantine consensus algorithm with linear complexity per bit agreed upon.

Related to the problem of agreement, we studied the performance of a probabilistic gossip algorithm in multi-channel wireless networks in the presence of an adversary. We considered a single-hop wireless network composed of n nodes. Each node has kf radios and the wireless spectrum is divided to kC channels, where k is an integer. At the beginning of each time slot, each node chooses kf channels uniformly at random out of kC channels and tunes to them till the end of the time slot. At each time

slot, a node decides to transmit on all of its radios with probability p, or receive on all of them with probability 1-p. At each time slot, the adversary chooses kf channels uniformly at random and jams them. Since the network is a single-hop network, if more than one node transmit on the same channel at the same time slot, the messages are corrupted and no useful data can be transferred to the nodes listening on the channel. Via simulations, we investigated the effect of changing k on the termination time of the gossip algorithm. In the gossip algorithm, each node begins the algorithm with an initial value and it attempts to transmit its initial value to the other nodes and receive the initial value of the other nodes. We consider all-to-all gossiping, in which the algorithm terminates whenever every node receives the initial value of all other nodes. We simulated the gossip algorithm for several different values of f and C to determine the optimum k that minimizes the termination time in each case.

(3) Achieving Exact Consensus in Presence of Directed Links
In MANET, due to the asymmetry in interference or channel characteristics, the available communication links may be asymmetric or directed links. When designing algorithms for such networks, one can either ignore the asymmetric links (using only the bidirectional links available), or attempt to exploit the asymmetric links to improve performance. In our work, we have explored strategies to exploit all available network links, including directed or asymmetric links. In particular, we have developed characterization of network graph topologies in which exact consensus is feasible on discrete quantities, despite the presence of adversarial (or compromised nodes). Such exact consensus algorithms are necessary to allow the nodes in the MANET to coordinate a common action (e.g., whether to collectively change the transmit power to a higher level or not). Informally, the necessary condition on the underlying graph, to be able to tolerate f compromised nodes, is as follows: if we remove any arbitrary set of f nodes in the network, and partition the rest of the network into sets of nodes L, R and C, then in the resulting graph, either the nodes in L have at least f+1 incoming external neighbors, or the nodes in R have at least f+1 incoming external neighbors. This condition generalizes on the notion of node connectivity. We show the sufficiency of the necessary condition constructively by developing an algorithm that can correctly solve the exact consensus problem.

By including additional conditions, beyond those necessary for exact consensus, it is also possible to obtain sufficient conditions for achieving broadcast over directed graphs in presence of adversarial nodes. In particular, the additional condition is to require 2f+1 disjoint directed paths from the source of the broadcast to each of the remaining nodes. The additional condition then can be used along with the above condition to allow the source node to transmit its state information to the other nodes in a consistent manner.

(4.4.4) Anonymous Communications in the Presence of Eavesdroppers

(1) A Statistical Framework for Source Anonymity in Sensor Networks
In certain applications, the locations of events reported by a sensor network need to remain anonymous. That is, unauthorized observers must be unable to detect the origin of such events by analyzing the network traffic. Known as the source anonymity problem, this problem has emerged as an important topic in the security of wireless sensor networks, with variety of techniques based on different adversarial assumptions being proposed. In this work, we present a new framework for modeling, analyzing and evaluating anonymity in sensor networks. The novelty of the proposed framework is twofold: first, it introduces the notion of “interval indistinguishability” and provides a quantitative measure to model anonymity in wireless sensor networks; second, it maps source anonymity to the statistical problem of binary hypothesis testing with nuisance parameters. We then analyze existing solutions for designing anonymous sensor networks using the proposed model. We show how mapping source anonymity to binary hypothesis testing with nuisance parameters leads to converting the problem of exposing private source information into searching for an appropriate data transformation that removes or minimize the effect of the nuisance information. By doing so, we transform the problem from analyzing real-valued sample points to binary codes, which opens the door for coding theory to be incorporated into the study of anonymous sensor networks. Finally, we discuss how existing solutions can be modified to improve their anonymity. Results accepted to appear in IEEE TMC.

(2) Minimizing Anonymous-Communication Vulnerabilities in a Multi-Path Network
In this work, given a multipath wireless network with covert and visible relays, we investigate how to analytically choose routes for each source-destination pair in order to offer maximum anonymity while maintaining a packet-loss constraint. We consider two types of packet-loss: link quality, determined by transmission power and the distance between nodes, and packets dropped by covert relays due to buffer constraints. We formulate the route selection problem within a rate-distortion framework, in which the fraction of flow allocated to each route is chosen to maximize the network anonymity without violating packet-loss constraints. We consider that the network is prefixed with fixed set of regular relays and mix nodes and the adversary can eavesdrop on all links. We then show that the flow allocation to minimize the information leakage to the adversary with packet loss constraints can be formulated as a Rate-Distortion optimization problem. These are preliminary results only. However, even at this early stage, we are able to show that the maximizing anonymity leads to the same optimization problem as capacity finding (Blahut-Arimoto family of algorithms) problem as the original problem is shown to be convex. The result for sources that operate independently was reported in IEEE ISIT 2012. We then consider the case that the sources may have partial information of each other and show that this can also leads to formulation that is mathematically similar to capacity finding algorithms. This is to be presented in the week of October 2012 at the 50th Allerton Conference in Urbana.

An important aspect of our project is the identification of the capabilities an adversary can exercise in attacking basic protocols. By identifying such capabilities, we can design secure protocols that withstand adversary attacks.

(4.4.5) Jamming-Protection Schemes

We developed four schemes that directly counter a jamming adversary. First, we developed a tree-based scheme that uses asymmetric knowledge between a sender and a receiver in order to counter an insider that jams broadcast messages. By sending each broadcast message both on a set of codes called a cover, and on a set of test codes, the sender can eventually isolate jammers on their own code, minimizing interference to legitimate nodes. Second, we developed a scheme for sleep scheduling that forces an energy-limited jammer to stay awake all the time, quickly depleting its battery power. Next, we developed JIM-Beam, an uncoordinated broadcast anti-jamming mechanism. Unlike prior work in keyless broadcast anti-jamming, JIM-Beam uses spatial diversity rather than frequency- or code-division, which has three major advantages. First, it gives strong security guarantees against a single adversary; second, it prevents wideband jamming because an attacker cannot distribute himself evenly in space; and finally, it allows users to send longer messages because reactive jamming in the spatial domain is much slower than reactive jamming in frequency or code. Finally, we developed SimpleMAC, a MAC protocol that is resilient to MAC-aware attacks. Specifically, SimpleMAC uses a jamming-resilient signaling scheme in place of the traditional control channel, and uses a transmitter strategy to share channel coordination information with a select group of nodes called the recipient list. SimpleMAC eventually converges to optimal performance, and almost immediately performs better than the no-MAC Nash equilibrium.

In the area of trusted core, we developed a bottom-up system to ensure epsilon-optimal performance in the long run. We started by using clock synchronization to detect wormhole attackers with equal capability as the normal users, and we expanded our protocol to allow for network-wide clock synchronization. We then developed a routing and scheduling mechanism that ensures epsilon-optimality over a sufficiently-long but bounded period of time. Finally, we extended our algorithm to work even when not all nodes start at the same time; in fact, we can have the network run for an unbounded amount of time before the last node joins, and still achieve epsilon-optimality for a fixed period of time after that node joins.

In vehicular networks, we explored the topic of trust and revocation, designing mechanisms for rapidly disseminating certificate revocation lists and exploring limitations on revocation. Our results show that vehicle mobility can effectively disseminate information over a large scale with little overhead. We have also taken strides in the deployment of VANETs, being the first work to characterize large-scale performance on actual mobility traces, as well as to determine the communications requirements for specific crash-avoidance applications. Our results provide a methodology for evaluating safety application performance requirements, and use intersection collision warning as an example. These results show that safety applications may have very different requirements from traditional data-driven network applications; for example, they may better tolerate losses, since each packet contains relatively little information, but may be much more sensitive to latency. We also developed power control mechanisms for avoiding congestion collapse in rush-hour traffic scenarios, and for limiting the privacy loss due to RF fingerprinting.

We developed a routing protocol, SEAR, for secure routing in ad hoc networks. We developed optimal secure localization schemes, showing the fundamental limits of combining the results of multiple verifiers when faced with a colluding adversary. We secured hybrid networks, ensuring that an attacker must always help the network achieve higher bandwidth with the help of the attacker, as compared to the case where the attacker were absent. We examined false channel condition reports, considering the impact on a variety of protocols when the adversary reports a channel condition either stronger or weaker than the actual condition. Finally, we developed CRAFT, which forces each flow to be TCP-friendly, even under a very weak deployment model, and even when routes are substantially asymmetric.

A significant accomplishment was the completion of the development of a complete clean-slate approach to secure wireless networking that was motivated by and commenced during this contract. There are extensions to be done, but we have completed the development of one complete clean-slate suite of protocols.

(4.4.6) Wiretap and Collaborative Jamming

The inherent openness of wireless communications makes it vulnerable to eavesdropping attacks. Following Shannon’s work on perfect secrecy, the secrecy problem is that of communicating a message through the Bob channel without conveying information about the message through the Eve’s channel. Later Wyner showed that when the Eve’s channel is a degraded version of the legitimate Bob’s channel, a positive information rate between Alice and Bob can be achieved.

The role of multiple antennas in wiretap channels has received much attention recently. For multi-antenna systems, assuming the channel state information is available at Alice, the available degree of freedom can be utilized to substantially degrade Eve’s effective channel. In "Robust beam forming for MISO wiretap channel by optimizing the worst-case secrecy capacity," and "Optimal transmit design for worst-case secrecy rate over uncertain MISO channels," we studied transmit design, without additional jammers’ help. The channel state information (CSI) of Eve and Bob is assumed to be imperfectly known. Given the uncertainty of the CSI, an optimal transmit covariance is solved to maximize a worst-case secrecy rate under the uncertainty.

Another idea of utilizing multiple antennas is to interfere Eve through artificial spatial noise, which is referred to as collaborative jamming or friendly jamming. The artificial noise can substantially degrade Eve’s channel quality with little or no harm to Bob’s

channel. Given perfect CSI, found an optimal joint design of transmit/jamming co-variances for MISO (multi-antenna Tx and jammer, single-antenna Rx Eve) wiretap channels (see A. W. Shi and J. Ritcey, "Cooperative transmit and jamming for maximizing secrecy rate of Gaussian MISO wiretap channels," IEEE Trans. Commun.), This was later extended to the case of MISOME (multi-antenna Tx and jammer, single-antenna Rx and multi-antenna Eve) wiretap channel (see J. Ritchey "Transmit beamforming and cooperative jamming for MIMOME wiretap channels," Asilomar Conf. on Signals Systems Computers, pp. 285-289, Nov. 2011). Given imperfect CSI, we proposed a new solution and its effectiveness has been demonstrated by several examples of location uncertainty.

(4.4.7) Interference Analysis for Large Networks

A wireless network can be viewed as a collection of nodes, located in some domain, and can be transmitters or receivers. As wireless networks become more pervasive with denser deployments, interference management has been becoming a defining issue of wireless network design. At a given time, several nodes transmit simultaneously, each toward its own receiver. The signal received from the link transmitter may be jammed by the signals received from the other transmitters. The geometry of the locations of the nodes plays a key role since it determines the signal to interference and noise ratio (SINR) at each receiver.

Stochastic geometry provides a natural way of defining and computing macroscopic properties of such networks, by averaging over all potential geometrical patterns for the nodes. The advantages of using stochastic geometry are: 1) performance metric can be exactly derived in some important cases, and tightly bounded in many others; 2) performance depends on fundamental network parameters, such as the densities of the underlying point processes. Design insights are obtainable from these performance expressions. A software tool is under development that generates and analyzes network interference models based on stochastic geometry.

Our goal is to characterize interference and the performance of multi-antenna receiver in large districted networks. Our work “Performance of MMSE multi-antenna receiver under hierarchical Poisson random fields of interferences," Asilomar Conf. on Signals Systems Computers, Nov. 2012, accepted, and “Performance of MMSE receiver: superposition property of multiple Poisson fields and its application to Poisson clustered interferers," IEEE Trans. Wireless Commun. (in prep) extends the performance analysis of multi-antenna minimum-mean-square-error (MMSE) receivers under Poisson point process (PPP) of interferers to that under more sophisticated Poisson spatial distributions, such as in-homogeneous PPP and Poisson clustered processes. These papers reveal an important fact that the effective interference caused by superposition of PPPs is the sum of the responses which would have been caused by each PPP individually.

(Please see Fig. 1 in the Attachment)

Fig. 1. (a) A realization of the Matern cluster process with parent density , expected children number and radius . Parent point process are homogeneously Poisson distributed with , and denotes the expected number of children per cluster. The children points are scattered independently identical distribution, around the parent point. Parent points are plotted in red ’+’ and children in blue ’o’ enclosed in dotted circles. (b) A realization of a homogeneous PPP with density . Note that the two processes have the same density .

(Please see Fig. 2 in the Attachment)

Fig. 2. Comparison of the simulated SINR outage and the theoretic SINR outage. We fix the density for better illustration (the resulting outage will vary within a small range). Matern process with is used as the children process. The SINR threshold is set to dB, and antenna number is . The theoretic results are plotted in solid curves, and the simulation results in ’+’. The comparison shows that the theoretic calculation is accurate.

Another paper "Distributed jamming for secure communication in a Poisson field of legitimate nodes and eavesdroppers," Asilomar Conf. on Signals Systems Computers, Nov. 2012 (accepted) investigates how cooperative jamming helps improve the secrecy throughput of large decentralized networks where the locations and channel state information (CSI) of eavesdroppers are both unknown. The spatial distribution of legitimate nodes including transmitter, receiver and helping jammers, and eavesdroppers are modeled as Poisson point process. A jamming protocol based on the RTS/CTS handshake of IEEE 802.11 standard is proposed for decentralized implementation. Our results show that multi-antenna helping jammers can significantly increase the secrecy of the network, compared to single-antenna jammers.

(Please see Fig. 3 in the Attachment)

Fig. 3. The secure throughput versus density of legitimate transmitters . Other network parameters are jammer density , eavesdropper density , transmitter power , and jammer power . The number of antennas for transmitter and eavesdropper are respectively.

(Please see Fig. 4 in the Attachment)

Fig. 4. The secure throughput versus jammer density . Other network parameters are transmitter density , eavesdropper density , transmitter power , and jammer power . The number of antennas for transmitter and eavesdropper are respectively.

(4.4.8) Interference Analyzer for a Multi-antenna Wireless Network IA-MWiN

This tool calculates performance metrics of multi-antenna nodes in a decentralized network in visualized manner, where the underlying network nodes are generated by Poisson point process and Poisson clustered processes. These nodes introduce interference into the ad-hoc and clustered ad-hoc network. This augments current methods in which the locations of the network nodes are given, or deterministic. The node locations are used to compute an interference map and the outage probability, which in term determines the connectivity of nodes.
The tool generates Poisson and Matern clustered nodes. An interference map can be created, conditional on the node locations, and fading model. The outage probability is computed when multi-antenna MMSE received is employed, and the number of antenna elements varied. Network connectivity is determined on anode-to-node basis. The outage results are used to threshold each pairwise link, connecting those in which the outage is below the threshold.

(5) Technology transfer

Collaboration and interaction with RDEC/CERDEC scientists and engineers, Dr. C.J. Graff and Mr. D.G. Yee, on modeling-simulation-validation of mobile ad-hoc networks, through a Phase II SBIR with AIMS, Inc. a small company. The collaboration also included transferring of modeling and simulation software to RDEC/CERDEC. During this reporting period work emphasized scheduling based MAC protocols for MANET, like the USAP protocol.

Collaboration with ARL scientists and engineers, Dr. B. Sadler and P. Yu, on the implications of traffic stochastic models of mobile wireless networks on network security and information assurance. During this period we continued the investigation of detection of wormhole attacks and the implications of various traffic models on attack detection performance.

We initiated research collaboration with Bosch Corporate R&D. Graduate student Shalabh Jain had an internship at Bosch Corporate R&D, where he worked in the area of Wireless Sensor networks security.

Technology Transfer

(1) List of papers submitted or published that acknowledge ARO support during this reporting period. List the papers, including journal references, in the following categories:

(a) Manuscripts submitted but not published

A. Clark, L. Bushnell, R. Poovendran, Joint Leader and Link Weight Selection for Fast Convergence in Multi-Agent Systems, submitted to IEEE ACC 2013.

A. Clark, Q. Zhu, R. Poovendran, T. Basar, "An Impact-Aware Defense against Stuxnet," submitted to IEEE ACC 2013.

Anand Muralidhar and P. R. Kumar, "Near-optimal quantization and linear network coding for relay networks," Submitted to IEEE Transactions on Information Theory. Submitted March 11, 2012.

G. Theodorakopoulos, J-Y. Le Boudec and J. S. Baras, "Selfish Response to Epidemic Propagation", accepted for publication in the *IEEE Transactions on Automatic Control*, to be published, February 2013.

Hemant Kowshik and P. R. Kumar, "Optimal Computation of Symmetric Boolean Functions in Col- located Networks." Submitted to IEEE Journal on Selected Areas in Communications: In-Network Computation: Exploring the Fundamental Limits. Submitted February 22, 2012.

I. Matei, J.S. Baras and V. Srinivasan, "Trust-Based Multi-Agent Filtering for Increased Smart Grid Security," journal paper, submitted, August 2012.

J.S. Baras and T. Jiang, "Composite Trust in Networked Multi-Agent Systems", journal paper, submitted, June 2012.

Jonathan Katz and Yehuda Lindell, Aggregate Message Authentication Codes, *IET Proc. Information Security*. Accepted pending revisions.

Kyoung-Dae Kim, Sayan Mitra and P. R. Kumar, "Bounded ε-Reach Set Computation of a Class of Deterministic and Transversal Linear Hybrid Automata." Submitted to IEEE Transactions on Automatic Control. May 15, 2012.

L. Tseng and N. H. Vaidya, "Iterative Approximate Byzantine Consensus under a Generalized Fault Model," to appear at International Conference on Distributed Computing and Networking (ICDCN), India, January 2013.

N. H. Vaidya, C. N. Hadjicostis, A. D. Dominguez-Garcia, "Robust Average Consensus over Packet Dropping Links: Analysis via Coefficients of Ergodicity," to appear at IEEE Control and Decision Conference, 2012.

Q. Zhu, A. Clark, R. Poovendran, T. Basar, SODEXO: A System Framework for Deployment and Exploitation of Deceptive Honeybots in Social Networks, under review at INFOCOM'2013.

S. Dov Gordon, Jonathan Katz, Ranjit Kumaresan, and Arkady Yerukhimovich. Authenticated Broadcast with a Partially Compromised Public-Key Infrastructure, Invited to a special issue of Information & Computation. Awaiting publication.

T. H. Kim, J. Ni, R. Srikant and N. H. Vaidya, "On the achievable throughput of CSMA under imperfect carrier sensing," IEEE/ACM Transactions on Networking (under review).

T. Jiang and J.S. Baras, "Collaboration in Networked Systems and Trust", journal paper, submitted, May 2012.

Tae Hyun Kim, Jian Ni, R. Srikant, N. H. Vaidya, "Throughput-Optimal CSMA with Imperfect Carrier Sensing," submitted to the IEEE/ACM Transactions on Networking.

Number of Manuscripts: 16

(b) Papers published in peer-reviewed journals

A. D. Dominguez-Garcia, C. N. Hadjicostis, N. H. Vaidya, "Resilient Networked Control of Distributed Energy Resources", IEEE Journal on Selected Areas in Communications, July 2012.

Arvind Seshadri, Mark Luk, and Adrian Perrig, "SAKE: Software attestation for key establishment in sensor network", Ad Hoc Networks Journal, Special Issue on Distributed Computing in Sensor Systems (DCSS), 9(6), 2011, pages 1059-1067.

B. Alomair and R. Poovendran, "E-MACs: Towards More Secure and More Efficient Constructions of Secure Channels," accepted to appear in IEEE Transactions on Computers.

B. Alomair, A. Clark, J. Cuellar, and R. Poovendran, "Scalable RFID Systems: a Privacy-Preserving Protocol with Constant-Time Identification," in IEEE Trans. Parallel and Distributed Systems, 23(8): 1536-1550 (2012)

B. Alomair, A. Clark, J. Cuellar, R. Poovendran, **"**Towards Statistical Framework for Source Anonymity in Sensor Networks," appeared in IEEE Transactions on Mobile Computing (TMC). DOI: 10.1109/TMC.2011.267

E. Athanasopoulou, L. Bui, T. Ji, R. Srikant and A. L. Stolyar, Back-Pressure-Based Packet-by-Packet Adaptive Routing in Communication Networks, IEEE/ACM Transactions on Networking, 2012 (to appear)

Haowen Chan, Hsu-Chun Hsiao, Adrian Perrig, and Dawn Song, "Secure Distributed Data Aggregation", Foundations and Trends in Databases, 3(3), 2011, pages 149-201.

Hemant Kowshik and P. R. Kumar, “Optimal Function Computation in Directed and Undirected Graphs.” IEEE Transactions on Information Theory, pp. 3407–3418, vol. 58, no. 6, June 2012.

I-Hong Hou and P. R. Kumar, “Queueing Systems with Hard Delay Constraints: A Framework and Solutions for Real-Time Communication over Unreliable Wireless Channels.” Queueing Systems: Theory and Applications, pp. 151-177, volume 71, issue 1, 2012.

I-Hong Hou and P. R. Kumar, “Real-Time Communication over Unreliable Wireless Links: A Theory and Its Applications.” IEEE Wireless Communications Magazine, vol. 19, issue 1, pp. 48–59, 2012.

J. Ghaderi and R. Srikant, “The Impact of Access Probabilities on the Delay Performance of Q-CSMA Algorithms in Wireless Networks,” IEEE/ACM Transactions on Networking, 2012 (accepted for publication)

J. Ni, B. Tan and R. Srikant, Q-CSMA: Queue-Length-Based CSMA/CA Algorithms for Achieving Maximum Throughput and Low Delay in Wireless Networks, IEEE/ACM Transactions on Networking, June 2012

Jerry T. Chiang, Jason J. Haas, Jihyuk Choi, and Yih-Chun Hu. Secure Location Verification Using Simultaneous Multilateration. IEEE Transactions on Wireless Networking 11(2):584-591. February 2012.

Kyoung-Dae Kim and P. R. Kumar, “A Real-Time Middleware for Networked Control Systems and Application to an Unstable System.” To appear in IEEE Transactions on Control Systems Technology.

Kyoung-Dae Kim and P. R. Kumar, “Cyber-Physical Systems: A Perspective at the Centennial.” Proceedings of the IEEE: Centennial Issue, pp. 1287–1308, vol. 100, no. 13, May 13th, 2012. (Invited Paper).

L. Jiang, M. Leconte, J. Ni, R. Srikant, J. Walrand, "Fast Mixing of Parallel Glauber Dynamics and Low-Delay CSMA Scheduling," IEEE Transactions on Information Theory, October 2012.

S. Zheng and J.S. Baras, "Sequential Anomaly Detection in Wireless Sensor Networks and Effects of Long Range Dependant Data", accepted for publication, to appear in the *Special IWSM Issue of Sequential Analysis (SQA)*, November 2012.

T. Bonaci, P. Lee, L. Bushnell, R. Poovendran, A Convex Optimization Approach for Clone Detection in Wireless Sensor Networks, appears in Pervasive and Mobile Computing. doi.org/10.1016/j.pmcj.2012.04.003

W. Shi and J. Ritcey, "Cooperative transmit and jamming for maximizing secrecy rate of Gaussian MISO wiretap channels," IEEE Trans. Commun., in press 2013.

Number of Papers published in peer-reviewed journals: 19

(c) Papers published in non-peer-reviewed journals or in conference proceedings

N/A

Number of Papers published in non peer-reviewed journals: 0

(d) Presentations

A. Perrig, SafeSlinger: Easy-to-Use and Secure Public-Key Exchange, keynote address at IEEE International Workshop on Trusted Collaboration (TrustCol), October 2012.

J.S. Baras, “COMPASS: Component-based Architectures for Systems Synthesis”, invited keynote address, *2012 MODPROD* conference, February 8, 2012, Linkoping, Sweden.

J.S. Baras, “Complex Network Problems Solutions via Greedy Hyperbolic Embedding,” invited lecture, *2nd NIST-Bell Labs Workshop on Large Complex Networks*, June 8, 2012.

J.S. Baras, “Cooperative Multi-Agent Systems and “Magical” Graphs,” distinguished lecture, Control Seminar Series, EECS Department, University of Michigan Ann-Arbor, March 9, 2012.

J.S. Baras, “Cooperative Swarms,” invited keynote lecture, *7th Annual Coordinated Sciences Laboratory Student Conference*, University of Illinois Urbana-Champaign, January 27, 2012.

N. H. Vaidya, Distinguished seminar, Department of Computer Science, SUNY at Stony Brook, February 2012.

N. H. Vaidya, Keynote talk, ACM 13th International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc), June 2012.

N. H. Vaidya, Keynote talk, ACM Workshop on Foundations of Mobile Computing (FOMC), July 2012.

N. H. Vaidya, Keynote talk, Joint ERCIM eMobility and MobiSense workshop, held at WWIC conference, Santorini, June 2012.

N. H. Vaidya, Keynote talk, The Forth IEEE International Workshop on Hot Topics in Mesh Networking (HotMesh), June 2012.

P. R. Kumar , Keynote Speaker, IEEE Wireless Communications and Networking Conference (WCNC 2013), Shanghai, China, April 7–10, 2013.

P. R. Kumar, Gene Brice Colloquium, Rice University, April 19, 2012.

P. R. Kumar, Keynote Speaker, 7th International Conference on Wireless Algorithms, Systems, and Applications (WASA 2012), Yellow Mountains, China, August 8–10, 2012.

P. R. Kumar, Keynote Talk at International Conference on Computing, Networking and Communications (ICNC), San Diego, January 29–31, 2013.

P. R. Kumar, NSF CISE Distinguished Lecture, February 6, 2013.

P. R. Kumar, Plenary Talk at Workshop on Network Science in Electrical Engineering and Computer Science, The International Centre for Theoretical Sciences (ICTS) of the Tata Institute of Fundamental Research, Bangalore, January 13, 2012.

P. R. Kumar, SIGMOBILE Outstanding Contribution Award Talk, MobiCom 2012: The 18th Annual International Conference on Mobile Computing and Networking, Istanbul, Turkey, August 22–26, 2012.

P. R. Kumar, Technical Plenary Speaker, IEEE International Conference on Communications (ICC 2012), Ottawa, Canada, June 10–15, 2012.

R. Srikant, Invited Lecture, Stochastic Networks Conference, June 2012.

Yih-Chun Hu, “Dynamic Defense for Wireless Networks,” Dynamic Defense Workshop, Sandia National Labs, Albuquerque, NM, September 2012.

Yih-Chun Hu, “Dynamic Defense for Wireless Networks,”Carnegie Mellon University, September 2012.

Yih-Chun Hu, “Jamming Defense for Wireless Networks”. Korea Advanced Institute of Science and Technology (KAIST), June 2012.

Number of Presentations: 22

(e) Non Peer-Reviewed Conference Proceedings publications (other than abstracts)

N/A

Number of Non Peer-Reviewed Conference Proceedings publications (other than abstracts): 0

(f) Peer-reviewed Conference Proceedings publications (other than abstracts)

A. Clark, L. Bushnell and R. Poovendran, Leader Selection for Minimizing Convergence Error in Leader-Follower Systems: A Supermodular Optimization Approach, in Wiopt'12, Paderborn, Germany, May 14th-18th 2012. WiOpt 2012 Best Paper Award.

A. Clark, Q. Zhu, R. Poovendran, T. Basar, Deceptive Routing in Relay Networks, in GameSec 2012, November 2012, Budapest, Hungary.

Amit Vasudevan, Bryan Parno, Ning Qu, Virgil D. Gligor, and Adrian Perrig, "Lockdown: Towards a Safe and Practical Architecture for Security Applications on Commodity Platforms," in Proceedings of the 5th International Conference on Trust and Trustworthy Computing (TRUST), June 2012.

Bryan Parno, Zongwei Zhou, and Adrian Perrig, "Using Trustworthy Host-Based Information in the Network," in Proceedings of the 7th ACM Workshop on Scalable Trusted Computing (STC), October 2012.

C. Yang, B. Alomair and R. Poovendran, Multipath Flow Allocation in Anonymous Wireless Networks with Dependent Sources, in 50th Allerton Conference October 1-5th 2012.

C. Yang, B. Alomair and R. Poovendran, Optimized Flow Allocation for Anonymous Communication in Multipath Wireless Network, IEEE ISIT 2012, Cambridge, Massachusetts, July 1-6, 2012.

Farhana Ashraf, Yih-Chun Hu, and Robin H. Kravets. Bankrupting the Jammer in WSN. Proceedings of the 9th IEEE International Conference on Mobile Ad-hoc and Sensor Systems (MASS 2012), IEEE, Las Vegas, Nevada. October 2012.

G. Liang and N. H. Vaidya, "Capacity of Byzantine Consensus in Capacity Limited Point-to-Point Networks," 4th International Conference on COMmunication Systems and NETworkS (COMSNETS), January 2012.

Guanfeng Liang and Nitin Vaidya "Byzantine Broadcast in Point-to-Point Networks using Local Linear Coding," ACM Symposium on Principles of Distributed Computing (PODC), July 2012.

Guanfeng Liang, Benjamin Sommer and Nitin Vaidya, Experimental Performance Comparison of Byzantine Fault-Tolerant Protocols for Data Centers, IEEE INFOCOM 2012.

J. Ghaderi and R. Srikant, "Flow-Level Stability of Multihop Wireless Networks Using Only MAC-Layer Information," Proc. WiOpt 2012.

J. Ghaderi, R. Srikant, Effect of Access Probabilities on the Delay Performance of Q-CSMA Algorithms, Proc. IEEE INFOCOM 2012.

J. Ghaderi, T. Ji, R. Srikant, Connection-Level Scheduling in Wireless Networks Using Only MAC-Layer Information, Proc. IEEE INFOCOM 2012 Mini-Conference.
J.S. Baras and T. Jiang, "Composite Trust in Networked Multi-Agent Systems", invited paper, *Proceedings 2012 American Control Conference*, pp. 3547- 3552, June 2012, Montreal, Canada.

Jerry T. Chiang, Dongho Kim, and Yih-Chun Hu. JIM-Beam: using Spatial Randomness to Build Jamming-Resilient Wireless Flooding Networks. Poster. Proceedings of the thirteenth ACM international symposium on Mobile Ad Hoc Networking and Computing (MobiHoc 2012), ACM, Hilton Head Island, South Carolina, June 2012, pp. 255-256.

M. Conti, R. Poovendran and M. Seccheiro, "FakeBook: Detecting Fake Profiles in On Line Social Networks," first International Workshop on Cyber Security of Online Social Network (CSOSN 2012), August 25th 2012, Istabul, Turkey.

I. Matei, J.S. Baras and V. Srinivasan, "Trust-Based Multi-Agent Filtering for Increased Smart Grid Security," *Proceedings 20th Mediterranean Conference on Control and Automation*, pp. 1266-1271, Barcelona, Spain, July 3-6, 2012.

Nitin Vaidya, Lewis Tseng, and Guanfeng Liang, "Iterative Approximate Byzantine Consensus in Arbitrary Directed Graphs," ACM Symposium on Principles of Distributed Computing (PODC), July 2012.

Parisa Haghani and Yih-Chun Hu. Power Control for Fair Dynamic Channel Reservation in VANETs. Proceedings of the 9th IEEE Communications Society Conference (SECON 2012), IEEE, Seoul, South Korea. June 2012.

Q. Zhu, A. Clark, R. Poovendran and T. Basar, Deceptive Routing Games, IEEE CDC 2012, December 10-14th 2012, Maui.

S. Jain and J.S. Baras, "Preventing Wormhole Attacks Using Physical layer Authentication", *Proceedings 2012 IEEE Wireless Communications and Networking Conference (WCNC2012)*, pp. 2712-2717, April 1-4, 2012, Paris, France.

S. Jain, T. Ta and J.S. Baras, "Wormhole Detection Using Channel Characteristics", *Proceedings 2012 IEEE International Conference on Communications (ICC'12), First International Workshop on Security and Forensics in Communication Systems (SFCS2012)*, June 2012, Ottawa, Canada.

Sang-Yoon Chang, Yih-Chun Hu, and Nicola Laurenti. Jamming-Resilient MAC-Layer Protocol for Wireless Channel Coordination. Proceedings of the Eighteenth Annual International Conference on Mobile Computing and Networking (MobiCom 2012), ACM, Istanbul, Turkey. August 2012.

Sang-Yoon Chang, Yih-Chun Hu, Hans Anderson, Ting Fu, and Evelyn Y. L. Huang. Body Area Network Security: Robust Key Establishment Using Human Body Channel. Proceedings of the 3rd

USENIX Workshop on Health Security and Privacy (HealthSec 2012), USENIX, Bellevue, Washington. August 2012.

T. Ta and J.S. Baras, "Enhancing Privacy in LTE Paging System Using Physical Layer Identification," *Proceedings 17th European Symposium on Research in Computer Security (ESORICS 2012), 7th International Workshop on data Privacy Management (DPM)*, Sept. 10-14, 2012, Pisa, Italy.

W. Shi and J. Ritcey, "Distributed jamming for secure communication in a Poisson field of legitimate nodes and eavesdroppers," Asilomar Conf. on Signals Systems Computers, Nov. 2012, accepted.

W. Shi and J. Ritcey, "Performance of MMSE multi-antenna receiver under hierarchical Poisson random fields of interferences," Asilomar Conf. on Signals Systems Computers, Nov. 2012, accepted.

Xin Zhang, Chang Lan, and Adrian Perrig, "Secure and Scalable Fault Localization under Dynamic Traffic Patterns," in Proceedings of the IEEE Symposium on Security and Privacy, May 2012.

Xin Zhang, Zongwei Zhou, Hsu-Chun Hsiao, Tiffany Hyun-jin Kim, Adrian Perrig and Patrick Tague, "ShortMAC: Efficient Data-Plane Fault Localization," in Proceedings of Networked and Distributed System Security Symposium (NDSS), February 2012.

Number of Peer-Reviewed Conference Proceedings publications (other than abstracts): 29

(e) Books

N/A

Number of Books: 0

(g) Papers presented at meetings, but not published in conference proceedings

N/A

(2) Scientific Personnel supported by this project and honors/awards/degrees received

Dr. Virgil Gligor (PI)	0.00
Dr. John S. Baras (co-PI)	0.08
Dr. Jonathan Katz (co-PI)	0.05
Dr. Carlos Guestrin (co-PI)	0.09
Dr. Rohit Negi, (co-PI)	0.17
Dr. Adrian Perrig (co-PI)	0.025
Dr. P.R. Kumar (co-PI)	0.045
Dr. Nitin Vaidya (co-PI)	0.13
Dr. Yih-Chun Hu (co-PI)	0.06
Dr. R. Srikant (co-PI)	0.083
Dr. R. Poovendran (co-PI)	0.04
Dr. Jim Ritcey (co-PI)	0.02

Graduate Students:

Andrew Clark (Graduate Research Assistant, partial support)	1.00
Chang-Han Jong (Graduate Research Assistant, partial support)	1.00
Chouchang Yang (Graduate Research Assistant, partial support)	1.00
J. Ghaderi (Graduate Research Assistant, partial support)	0.125
Phillip Lee (Graduate Research Assistant, partial support)	1.00
S. Jain (Graduate Research Assistant, partial support)	0.14
T. Ta (Graduate Research Assistant, partial support)	0.63
V. Ivanov (Graduate Research Assistant, partial support)	0.75
X. Liu (Graduate Research Assistant, partial support)	0.75
Rui Wu (Graduate Research Assistant, partial support)	0.125
Chong Jiang (Graduate Research Assistant, partial support)	0.125
Siva Maguluri (Graduate Research Assistant, partial support)	0.19
Bo Tan (Graduate Research Assistant, partial support)	0.125

Post Doctoral Fellows:

Kyoung-Dae Kim	0.08
P. Purkayastha	0.15
Seung Geol Choi	0.75
V. Ivanov	0.25

The following graduate students completed their degrees during the reporting period.

Chang Han Jong, PhD

Bo Tan, PhD

Shanshan Zheng, PhD
Tamara Bonaci, MS
Vladimir Ivanov, PhD

Guanfeng Liang, PhD
Vijay Raman, PhD
Jerry T. R. Chiang
Dongho Kim
Jihyuk Choi

Technical Support

N/A

Honors and Awards received

J.S. Baras, “COMPASS: Component-based Architectures for Systems Synthesis”, invited keynote address, *2012 MODPROD* conference, February 8, 2012, Linkoping, Sweden.

P. R. Kumar, ACM SIGMOBILE Outstanding Contribution Award, 2012. For “pioneering contributions to the foundations of asymptotic performance analysis of large scale wireless networks.”

P. R. Kumar, Distinguished Alumnus Award, IIT Madras, 2012.

R. Srikant , Distinguished Lecturer, IEEE Communications Society, 2012-2013

WiOpt 2012 Best Paper Award, http://wi-opt.cs.upb.de/WiOpt_2012/Home.html

(3) Report of Inventions *(*Titles of Patents disclosed during the reporting period)

V. Ivanov and J.S. Baras, “Method and Apparatus for Authenticating Area Biometric Scanners,” Patent Application filed May 24, 2012.

Number of Patents disclosed during the reporting period: 1

Patents Awarded during the reporting period

"Novel Topology Selection and Broadcast Mechanism for Link State Stable Path Routing", (J.S. Baras, K. Somasundaram, K. Jain, V. Tabatabaee), Allowed September 2012.

V. Ivanov and J.S. Baras, “Method and Apparatus for Authenticating Biometric Scanners,” Notice of Allowance, Sept. 14, 2012.

Number of patents awarded: 2

(4) Scientific progress and accomplishments (Description should include significant theoretical or experimental advances)

Our work continued along the same broad directions of the overall research theme of this MURI, namely the design and operation of reliable and secure tactical MANET. The emphasis of our research was on the discovery and development of methods and algorithms that can unify the investigation of resiliency and security for MANETs. With this emphasis, we investigated fundamental problems addressing the characterization, properties and design of the *Trusted Core* of a MANET. More specifically we investigated several research problems in the context of Tasks 1 – 4 (**Thrusts 1-4**).

(4.1) Thrust 1: Design of Dependable Trusted Core of MANET

Several efforts were made to realize the vision of the trusted core sub-network. More specifically, our focus was on Message and Device Authentication in MANETs. In this area, we pursued the following specific topics:

(4.1.1) Message, Node, and Device Authentication in MANETs

(1) Authentication of Fingerprint Scanners

To counter certain security threats in biometric authentication systems, particularly in portable devices (e.g., phones and laptops), we have developed a technology for automated authentication of fingerprint scanners of exactly the same type, manufacturer, and model. The technology uses unique, persistent, and unalterable characteristics of the fingerprint scanners to detect attacks on the scanners, such as detecting an image containing the fingerprint pattern of the legitimate user and acquired with the authentic fingerprint scanner replaced by another image that still contains the fingerprint pattern of the legitimate user but has been acquired with another, unauthentic fingerprint scanner. The technology uses the conventional authentication steps of enrolment and verification, each of which can be implemented in a portable device, a desktop, or a remote server. The technology is extremely accurate, computationally efficient, robust in a wide range of conditions, does not require any hardware modifications, and can be added (as a software add-on) to systems already manufactured and placed into service. We have also implemented the technology in a demonstration prototype for both area and swipe scanners. Further, we have demonstrated how this physical layer technique can be combined with other physical layer techniques like TPM, MTM, TCN and modulation watermarking tags to strengthen considerably the security of mobile wireless devices and networks.

(4.1.2) Securing Neighborhood Discovery in MANETs using Physical Layer Authentication

Mobile ad-hoc networks (MANETs) are a key enabler of pervasive computing. Constrained resources in mobile stations make it critical for nodes to be able to cooperate to enhance communication and computation capabilities. However, the wireless and dynamic nature of the links presents easy attack vectors for adversaries. The ability to securely discover and identify neighboring nodes (secure ND) is a fundamental building block for such networks. Even a relatively weak adversarial relay has the capability of distorting the network view and diverting significant amount of traffic. This can cause significant performance degradation. In our work, we utilized a physical layer authentication scheme to secure neighborhood discovery against adversarial relays. Our proposed method incurs little performance overhead and requires no additional hardware. We developed analytical and performed simulation based performance evaluations of the security of our scheme. We also demonstrated that the scheme can be used efficiently to prevent wormhole attacks.

(4.1.3) Round-efficient broadcast authentication and signatures in general and specialized network topologies

We studied mechanisms for round-efficient broadcast authentication protocols for fixed topology classes. Although numerous efficient broadcast authentication techniques exist, we have identified significant improvements for authentication latency for existing protocols in specific communication topologies. Moreover, we have proposed new approaches for broadcast authentication. These are exciting results, because broadcast authentication has been studied for two decades. Our new results demonstrate lower bounds for broadcast authentication in various topologies, as well as protocols that match or get very close to these bounds.

More specifically, we consider resource-constrained broadcast authentication for n receivers in a static, known network topology. There are only two known broadcast authentication protocols that do not use asymmetric cryptography, one-time signatures, multi-receiver MACs, or time synchronization: the Guy Fawkes protocol by Anderson et al., and a protocol based on secure aggregation by Chan and Perrig. Both these protocols require three passes of a message front

traversing the network. We investigate whether this amount of interaction can be improved efficiently for specific common topology classes, namely, linear topologies, tree topologies and fully connected topologies. We show modifications to the protocols allowing them to complete in just two passes in the linear and fully connected cases with a small constant factor increase in per-node communication overhead, and a further optimization that achieves the equivalent of just a single pass in the linear case with O(log(n)) increase in per-node communication overhead. We also prove new lower bounds for round complexity, or the maximum number of consecutive interactions in a protocol. We show that protocols with efficient per-node communication overhead (polylogarithmic in n) must require at least 2*log(n) rounds in any topology; this implies that our two-pass protocol in the fully-connected topology requires the fewest possible passes, and this bound is asymptotically tight for the full-duplex communication model. Furthermore, we show that communication-efficient protocols must take asymptotically more than 2*log(n) rounds on trees; this implies that that there are some tree topologies for which two passes do not suffice and the existing three-pass algorithms may be optimal.

These new results will likely have a significant impact on the design of secure network protocols. For example in the case of secure routing protocols, our approach for broadcast authentication in linear topologies can enable efficient authentication along a network path. We will investigate the application of these protocols in the context of our project.

(4.2) Thrust 2: Adaptive Protocol Monitoring for Efficiency and Dependability

(4.2.1) Routing Protocol Monitoring for Wormhole Detection

The potential applications and pervasive nature of mobile ad-hoc networks (MANETs) has made them an attractive target for attackers. The wireless medium of communication coupled with constrained resources enable attacks, which can be executed by a weak adversary. A wormhole is one such attack, which poses considerable threat, particularly to routing protocols. In this attack, two adversarial nodes create a low latency out-of-band link (wormhole), either via external hardware or tunneling through network nodes. The attackers thus provide a path with low hop count. Typical MANET routing algorithms, such as AODV and DSR, select such links for routing, allowing the adversary to draw large amounts of network traffic. Such high traffic links under adversarial control can cause significant leakage of network secrets, performance degradation and congestion in the network. In our work, we devised a novel scheme for detecting a wormhole by utilizing the inherent symmetry of electromagnetic wave propagation in the wireless medium. We demonstrated the loss of this symmetry in the case of a wormhole attack and proposed a method to detect and flag the adversary. We modified the insecure neighborhood discovery to incorporate authentication. We further extended this scheme to a trust system with low overhead.

Our scheme operates independent of the higher layer MAC and routing protocols. We assume the existence of some form of contention management scheme for access to the wireless channel. For authentication during the neighborhood discovery phase, the scheme will perform well with any MAC and higher layer protocol. However, to build trust systems, we require the packet reception to be acknowledged. Thus, any MAC protocol that ensures instant feedback after packet reception will suffice, for example, the 802.11 MAC. We assumed the adversarial behavior to be limited to relaying and any offline attacks. In case of a relay with the capability to modify the packets, we can couple our scheme with any higher layer protocol used to ensure integrity of the messages in the network. For example, any form of a message authentication code will serve this purpose. It should be noted that hidden wormholes typically cannot be thwarted by higher layer cryptographic schemes. The benefits of our scheme thus complement the higher layer cryptographic methods.

(4.2.2) Trusted Multi-Agent Cores in Distributed Inference and Control

We investigated fundamental problems of modeling and representation of distributed multi-agent inference and decision making problems and we developed a new general model for such systems that involves constrained coalitional games and several interacting dynamic multigraphs, with nodes and links annotated by weights (including vector and logical ones). The framework emphasizes observables, partial information and de-emphasizes state models. The approach is justified on foundational principles. We then proceeded to develop a detailed model that involves models of the collaboration and communication multi-graphs between the agents. We developed new optimization-based analytics and new stochastic models for these problems that allow a careful analysis of the impact of the communication topology on performance. We also investigated extensions to algebraic structures involving partially ordered semirings, which allow the incorporation of logic-based strategies. We further extended the framework to allow the incorporation of adversaries including collaborating ones.
To provide a more fundamental understanding on how to model and analyze multi-agent systems in the presence of adversaries, we investigated distributed inference and learning problems in networked systems with adversaries. We analyzed the effects of adversarial attacks on the solutions and characterized the solution robustness and resiliency as functions of network topology and adversary distribution. We demonstrated that the existence of a small "trusted core" that provides substantial improvements to solution robustness and resilience. We characterized these improvements as functions of the degree of trust, connectivity and location of trusted nodes. We introduced value-directed graphs with weighted nodes as our model for composite trust, and included not only numerical weights, but also constraints. We showed that the semiring-based constraint satisfaction problem (SCSPs) framework can serve as the unified model to investigate trust relation establishment and its effect on performance of trusted cores of multiple agents.

As an application of these fundamental concepts and constructs we considered ad hoc networks, which rely on the mutual cooperation among individual nodes to achieve network-wide objectives. However, individual nodes may behave selfishly in order to maximize their own benefits without considering the global benefits of the network. One approach to incentivize nodes cooperation for better global benefits is to establish trust relations among nodes to guide their decision making. In our research work during this period, we developed a game theoretic analysis for the efficiency of establishing trust for improving node cooperation. The trust relations among nodes are modeled as a trust-weighted network, and we studied a graphical game in this network where the nodes' payoffs are affected by their trust relations. We characterized the Nash equilibrium and the social optimum of this game and showed that the game efficiency has a close relationship to the Bonacich centralities of nodes in the trust-weighted network. Furthermore, we proposed an improvement of game efficiency by introducing heterogeneous resources to nodes according to their centralities. We provided both experimental and theoretical analysis on the improvement of the game efficiency.

(4.3) Thrust 3: Network Utility Maximization

(4.3.1) An Axiomatic Clean Slate Approach To Secure Wireless Networking

Traditionally, wireless network protocols have been developed for performance. Subsequently, as attacks are identified, patches or defenses are developed. This leads to an "arms race," where one is never confident about what other vulnerabilities may be exposed in the future. We seek to reverse this process. We identify a set of axioms, under which we develop an ***optimally secure utility maximized network*.** Our results rest on the axioms, and can be attacked only to the extent that the axioms can be challenged. We present a complete suite of protocols, taking a wireless network all the way from startup to optimality. These protocols are not just individually secure, they are holistically secure, that is, there are no gaps between them that can be attacked.

Consider a group of wireless nodes some of which are good, and the rest, bad. The good nodes seek to form a functioning wireless network, operating at some measure of utility. The bad nodes know the identities of the good nodes but not conversely. Moreover, unlike their good counterparts, the bad nodes are capable of fully centralized cooperation and collusion. On the other hand, the good nodes arrive on the scene unsynchronized, uncoordinated and ignorant of the others' intentions.

We introduce a distributed protocol that enables the good nodes to proceed all the way from primordial birth to a Min-Max utility optimal network, where the minimization is over all bad behaviors of the bad nodes, and the maximization is over all protocols followed by the good nodes. That is, the good nodes form a functioning, reliable network from startup, in the face of any sustained cooperative attack mounted by the bad nodes. We show that the protocol overhead occupies an arbitrarily small fraction of the total operating lifetime. We prove that no other protocol can attain a higher level of utility.

Our protocol supersedes a considerable amount of previous work that deals with several classes of attacks such as the following: man-in-the middle, wormholes, dropping packets, Byzantine behaviors, disruption of timing events, presenting false topologies, etc. More importantly, this protocol obviates the need to identify all of the other types attacks that can potentially be carried out by colluding malicious nodes, for there are many. Instead, this protocol forces the malicious nodes to just one of two behaviors: comply with the protocol as a proper participant, or jam from the outside.

(4.3.2) Multi-criteria Optimization, Resilience, and Robustness

Network utility maximization suggests a decomposition by which congestion, routing, MAC and other layers of the network protocol stack naturally arise from duality theory. In this project, our goal has been to study the resilience and robustness of the MAC protocols. In particular, we have been interested in the resilience and robustness of the protocol to the following factors:

(i) Limited communication and computational capability of the nodes
(ii) Imperfect carrier sensing
(iii) Impact of dynamics in the network topology
(iv) Impact of dynamics in the flow composition in the network.

The main feature of the protocol developed by us is the use of queue length information in assigning weights to links in the network. This assignment of weights also allows us to easily incorporate trust metrics developed in other parts of this MURI project in our MAC protocol. For example, our protocol continues to perform well if the link weights are multiplied by a constant. Thus, if a trust metric is available, we could multiply the link to boost or inhibit the use of a link by the MAC protocol. We now summarize our accomplishments in each of the four categories above.

(i) It had been shown by others that CSMA-type random access algorithms can achieve the maximum possible throughput in ad hoc wireless networks. However, these algorithms assume an idealized continuous-time CSMA protocol where collisions can never occur. In addition, simulation results indicate that the delay performance of these algorithms can be quite bad. On the other hand, although some simple heuristics (such as distributed approximations of greedy maximal scheduling) can yield much better delay performance for a large set of arrival rates, they may only achieve a fraction of the capacity region in general. In this project, we proposed a discrete-time version of the CSMA algorithm. Central to our results is a discrete-time distributed randomized algorithm which is based on a generalization of the so-called Glauber dynamics from statistical physics, where multiple links are allowed to update their states in a single time slot. The algorithm generates collision-free transmission schedules while explicitly taking collisions into account during the control phase of the protocol, thus partially relaxing the perfect CSMA assumption. More importantly, the algorithm

allows us to incorporate mechanisms which lead to very good delay performance while retaining the throughput-optimality property.

(ii) In (i) above throughput-optimality is established under the assumption that each link can precisely sense the presence of other active links in its neighborhood. Going further, we investigated the achievable throughput of the CSMA algorithm under imperfect carrier sensing. Through the analysis on both false positive and negative carrier sensing failures, we show that CSMA can achieve an arbitrary fraction of the capacity region if certain access probabilities are set appropriately. To establish this result, we use the perturbation theory of Markov chains.

(iii) In (i) and (ii) above, each link of the wireless network has two parameters: a transmission probability and an access probability. The transmission probability of each link is chosen as an appropriate function of its queue length, however, the access probabilities are simply regarded as some random numbers since they do not play any role in establishing the network stability, other than in dealing with imperfect carrier sensing. In this paper, we show that the access probabilities control the mixing time of the CSMA Markov chain and, as a result, affect the delay performance of the CSMA. In particular, we derive formulas that relate the mixing time to access probabilities and use these to develop the following guideline for choosing access probabilities: for each link I should choose I set its access probability equal to 1/(d+1), where d is the number of links which interfere with link i. Simulation results show that this choice of access probabilities results in good delay performance.

(iv) We have primarily focused on the resilience and robustness of the MAC protocol to the dynamics of flow composition in the network. It is by now well-known that wireless networks with file arrivals and departures are stable if one uses a class of congestion control mechanisms called alpha-fair congestion control mechanisms, and back-pressure based scheduling and routing. In recent work, we have shown that stability can be ensured even with very simple congestion control mechanisms, such as a fixed window size scheme, which limits the maximum number of packets that are allowed into the ingress queue of a flow. A key ingredient of our result is the use of the difference between the logarithms of queue lengths as the link weights. This is exactly the weight function used in our MAC protocol. The results suggests that the MAC protocol alone leads to considerable resiliency in the network protocol stack, and stability is maintained even if different flows in the network use different transport-layer protocols, and even if the flows in the network dynamically change with time.

(4.3.3) Multi-metric Shortest Path Algorithms for Secure Routing

We completed the investigation of partially ordered semiring frameworks for robust pruning in MANET routing and hierarchical routing as well as multi-metric problems in multi-scale networks and analyzed connections to the Algebraic Stochastic Shortest Path Problem which led to new solutions and algorithms for pruning and topology dissemination for MANET. We introduced and investigated the stable path topology control problem for link-state routing in mobile multihop networks. We adopted a graph pruning approach to reduce the broadcast storm problem for link state routing: by selecting a subset of the graph topology to be broadcast, the broadcast storm can be reduced. Several of the pruning mechanisms proposed in the literature are distributed localized algorithms. One important metric for routing in wireless multi-hop networks is path stability. Although path stability has been studied for many reactive distance vector schemes, there is little work that addresses topology control for stable paths in link state routing. We introduced a new topology control algorithm that guarantees stable path routing: a mechanism that prunes the initial topology (to reduce the broadcast storm) while guaranteeing that the stable paths (for unicast routing) from every host to any target station are preserved in the pruned topology. We developed a multi-agent optimization framework where the decision policies of each agent are restricted to local

policies on incident edges and independent of the policies of other agents. We showed that under a condition called the *positivity condition*, these independent local policies preserve the stable routing paths globally. We also provided an efficient and distributed algorithm, which we call the *Stable Path Topology Control Algorithm*, to compute this local policy that yields a pruned graph. We applied these analytic methods to develop provably secure MANET routing protocols, where the two metrics (e.g. link metrics) for example can be for example *path delay* and *path trust*.

(4.3.4) Selfish Misbehavior in Scheduling Algorithms of Wireless Networks:

We consider the problem of selfish misbehavior in scheduling algorithms of wireless networks. The wireless medium is a shared medium and simultaneous data transmission over conflicting links is not desirable. A scheduling algorithm determines the set of links to be activated at any given time such that the interference constraints of the wireless network are not violated. Scheduling algorithms are often designed under the assumption that network users will follow the algorithm specifications properly. We considered two scenarios in which a selfish user misbehaves from the protocol in order to achieve better performance such as higher throughput or less delay. The primary goal of a selfish user is to improve its own performance, but its greedy misbehavior usually results in performance degradation of honest hosts. In particular, we consider selfish misbehavior in cross-layered rate control algorithm of wireless networks. A cross-layered approach to rate control is a mechanism in which the network jointly optimizes data rates of the users and link schedules. Cross-layered rate control algorithm of wireless networks is equivalent to a utility optimization framework, which can be decomposed into two components: rate control at the transport layer and scheduling at the MAC layer. We present a scenario in which a selfish user misbehaves in order to obtain higher throughput. We consider a wireless network in which the link capacities change over time and users of the network are involved in the process of measuring and estimating the link capacities. A selfish user may misbehave in this process and mislead the scheduler about the actual value of its link capacity. We find an equivalent optimization framework that captures misbehavior pattern of the selfish user. We impose a cost term on the utility function of the users in order to prevent such a selfish misbehavior. Penalties and rewards provide strong mechanisms for solving network problems and achieving performance objectives. We find the cost term in a network in which the conflict graph is a complete graph. In this case, at each time instance, at most one link can be activated for data transmission. We determined, for this network, which cost function prevents selfish misbehavior. We also developed a heuristic for identifying a cost function in an arbitrary network.

(4.4) Thrust 4: Threat Modeling Detection and Defense in MANETs

(4.4.1) Detection of Adversary-Induced Faults

In MANETs, which are multi-hop wireless networks, the path between a source and a destination may often contain multiple hops, and data packets are relayed on the different hops from the source to the destination. This multi-hop nature makes the wireless networks subject to adversary-induced faults and tampering attacks; e.g., a compromised or misbehaving node can tamper packets it forwards. We have investigated mechanisms for the detection of such tampering attack in wireless networks.

(1) Watchdogs with Source Coding:

The well-known watchdog mechanism is a monitoring method used for ad hoc networks, and is the basis of many misbehavior detection algorithms, and trust or reputation systems. The basic idea of the watchdog mechanism is that the network nodes (acting as watchdogs) police their downstream neighbors locally, using overheard messages, in order to detect misbehavior. If a watchdog detects that a packet is not forwarded within a certain period, or is altered by its neighbor before forwarding, it deems the neighbor as misbehaving. When the misbehavior rate for a node surpasses certain

threshold, the source is notified and subsequent packets are forwarded along routes that exclude the misbehaving node. The main challenge for the watchdog mechanism is the unreliable wireless environment. Due to channel fading and interference, even when the transmitter and the watchdog are both within communication range, the watchdog may not be able to overhear every transmission, and therefore may be unable to determine whether packets were tampered. So it is possible that the watchdogs will not detect an attacker.

To mitigate the misbehavior of the malicious nodes, a watchdog mechanism must achieve the following two goals: malicious behavior in the network should be detected with high probability, and, in the absence of an attack, the throughput under the detection mechanism should be comparable to the throughput without detection. These two goals seem to be conflicting. On the one hand, more redundancy is required to improve the probability of detection. On the other hand, higher throughput requires redundancy to be reduced. However, we have showed that both goals can be achieved simultaneously by introducing error detection coding to the watchdog mechanism. We have developed a computationally simple scheme that integrates source error detection coding and the watchdog mechanism. We showed that by choosing the coding scheme properly, a misbehaving node would be detected with high probability, without degrading the throughput much, even if the watchdog can only overhear a fraction of the packets. We also developed a protocol that identifies the misbehaving node using two watchdog nodes per potentially misbehaving relay node. We also showed that, together with source error detection coding, the probability of correctly locating the malicious node can be made close to one.

We further extended this work to explore the impact of packet tampering, and the use of watchdogs, on TCP flows. In particular, we observed the phenomenon of watchdog-induced packet losses with TCP flows. Such losses can occur even in the absence of packet tampering by an attacker, when the notifications from the watchdog are delayed. The TCP receiver, due to such a delayed notification, will not be able to send a TCP ACK, potentially causing the TCP sender to timeout. Such a timeout causes the TCP sender to behave as if a packet is lost along the route, and it responds by performing congestion control, degrading TCP throughput. We have developed simple mechanisms to reduce the impact of such watchdog-induced packet losses, and evaluated the ability of our mechanisms to improve performance.

The watchdog mechanism can also be applied in the case when the MANET uses multiple channels. With the use of multiple channels, it is beneficial for the different nodes to transmit on different channels, to improve performance. However, such a channel usage can also reduce the opportunities for the nodes to watch each other's transmissions to detect misbehavior. We identified this trade-off, and developed a strategy that can yield the performance benefits of multiple channels, while also attempting to ensure that watchdogs can observe forwarded packets for detection of misbehavior.

(2) Secure Capacity of Information Networks Without Monitoring

We have also investigated the secure capacity of information networks under tampering attacks. In particular, we studied the maximum achievable rate for a source-destination pair such that any attack by a compromised node can be detected. Significant research effort has been previously directed towards analysis of capacity with linear network coding. It has been shown by others that the error detection capacity with linear network coding is C-Z where C is the minimum cut between the source and the destination and Z is the mincut between the adversary and the destination. However, the adversary model assumed by this past work is a link-level model in which the adversary can attack any Z links in the network. In reality, the adversary is often node-level in the sense that the adversary captures a node and can attack all the out-going links from that node. We first characterized the secure capacity with end-to-end error detection, assuming that no intermediate nodes in the network monitor their neighbors (that is, no watchdogs). We restrict ourselves to the case when coding is only performed by the source, or by the neighbors of the source, and the

remaining nodes optionally duplicate and forward the packets they receive. The problem of characterizing the achievable rates can then be formulated as an optimization problem. The solution of the optimization problem not only yields the maximum achievable rate, but also a routing strategy to achieve this rate. We also investigated the secure capacity with monitoring in which intermediate nodes can watch or monitor their neighbors and compare the packets they overhear. We showed that there exist networks in which secure capacity with such monitoring can be arbitrarily larger than that without monitoring.

We also considered an approach wherein a traffic flow is carried on multiple node-disjoint routes, allowing different packets from the same flow to travel different subsets of such routes. Specifically, we considered the case where the flow may use any two of three disjoint routes for each packet on the flow. The goal now is to determine the best set of routes to be used for each packet, and the scheduling policy that can optimize the rates of the various flows. We achieved this goal by maintaining multiple virtual queues for each flow: one queue is for data that has not yet been sent to any receiver, and the other three queues are for data that has been sent on one of the disjoint paths. Virtual links with appropriate rates are added between the various queues, so as to capture the replication requirement correctly. We then use the utility optimization framework to develop a congestion control algorithm and a backpressure-based scheduler that can optimize the network utility under the disjoint route requirement. This approach can be generalized to more complex networks.

(4.4.2) Network Localization of Adversary Induced Faults

In our previous work, we showed that the ability of the trusted core (TC) to maintain effective communication despite link uncertainty (e.g., channel fading, interferences, environment obstacles, fluctuating weather patters), changing network topology and dynamic node membership, suggests two complementary approaches to adaptive communication protocol design: (1) stochastic network modeling and (2) machine learning. A central goal of our project is to achieve highly available network communication in the presence of active adversaries. In particular, we would like to provide lower bounds for network availability, such that the network can guarantee to provide useful throughput even in the presence of adversaries. We have considered several approaches to achieve these properties, and during the project we have designed two schemes, one based on cryptographic approaches and the other based on trusted hardware. Leveraging efficient fault localization, we can devise a network architecture that provides guaranteed throughput, based on the observation that attackers face a dilemma: if they misbehave and cause damage beyond a certain threshold, the fault localization will detect them and they will be removed; but if they cause less damage than the threshold, then they provide a useful level of bandwidth. Consequently, the network will provide a guaranteed level of throughput despite the adversaries.

We have three major accomplishments in the localization of adversary-induced faults: ShortMAC, DynaFL, and Assayer.

(1) ShortMAC

Previous fault localization protocols could not achieve a practical tradeoff between security and efficiency and they require unacceptably long detection delays, and require monitored flows to be impractically long-lived. We designed an efficient fault localization protocol called ShortMAC, which leverages probabilistic packet authentication and achieves 100-10000 times lower detection delay and overhead than related work. We theoretically derive a lower-bound guarantee on data-plane packet delivery in ShortMAC, implement a ShortMAC prototype, and evaluate its effectiveness using the SSFNet simulator and Linux/Click routers. Our implementation and evaluation results show that ShortMAC causes negligible throughput and latency costs while retaining a high level of security.

(*2) DynaFL*

Compromised and misconfigured routers are a well-known problem in ISP and enterprise networks. Data-plane fault localization aims to identify faulty links of compromised and misconfigured routers during packet forwarding, and is recognized as an effective means of achieving high network availability. Existing secure fault localization protocols are path-based, which assume that the source node knows the entire outgoing path that delivers the source node's packets and that the path is static and long-lived. However, these assumptions are incompatible with the dynamic traffic patterns and agile load balancing commonly seen in modern networks. To cope with real-world routing dynamics, we propose the first secure neighborhood-based fault localization protocol, DynaFL, with no requirements on path durability or the source node knowing the outgoing paths. Through delayed key disclosure, DynaFL incurs little communication overhead and a small, constant router state independent of the network size or the number of flows traversing a router. In addition, each DynaFL router maintains only a single secret key, which based on our measurement results represents 2-4 orders of magnitude reduction over previous path-based fault localization protocols.

(3) Assayer

As hardware support for improved end-host security becomes ubiquitous, it is important to consider how network security and performance can benefit from these improvements. If portions of each end-host can be trusted, then network infrastructure no longer needs to arduously and imprecisely reconstruct data already known by the end-hosts. Through the design of a general-purpose architecture we call Assayer, we explore issues in providing trusted host-based data, including the balance between useful data and user privacy, and the tradeoffs between security and efficiency. We also evaluate the usefulness of such information in several case studies. We implement and evaluate a basic Assayer prototype. Our prototype requires fewer than 1,000 lines of code on the end-host. End-hosts can annotate their outbound traffic in a few microseconds, and these annotations can be checked efficiently; even packet-level annotations on a gigabit link can be checked with a loss in throughput of only 13.1%.

(4.4.3) Consensus and Approximate Agreements in the Presence of the Adversary

(1) Reaching Approximate Consensus

In the MANETs, and in other networks as well, the different nodes in the network may need to agree on a consensus on a real-valued quantity as a function of values sensed or proposed by the different nodes in the network. For instance, clock synchronization is an example of this problem, wherein each node in the network proposes a value for the current time, and then the nodes must agree on a common notion of the current time as a function of the proposed values. Similarly, each node in the network may sense external parameters such as the temperature, and the nodes need to collaboratively agree on a common notion of the external temperature. We consider this problem in a setting wherein an adversary may have compromised some of the nodes in the network. The compromised nodes can attempt to cause the state of the good nodes to diverge. To tolerate such a threat, we have developed an iterative algorithm that can allow the good nodes to reach consensus on real-values parameters despite the presence of a bounded number of adversarial nodes. We have also characterized properties of the underlying directed graph topology that are necessary to be able to tolerate a specified number of compromised nodes. The iterative algorithm only requires local communication between each node and its neighbors, and allows directed or asymmetric links, which can occur in wireless networks due to asymmetries in interference or channel characteristics. The iterative algorithm uses very simple iterative computational steps to achieve its objective. We prove that when the underlying network graph satisfies certain graph-theoretic sufficient properties, the algorithm will achieve convergence to a valid value, in the convex hull of inputs at the good nodes, despite misbehavior by compromised nodes, when the number of such nodes does not exceed a specified threshold.

In wireless networks, due to transmission errors, the links have a lossy behavior. We have explored the impact of such lossy links on the performance of iterative consensus algorithms that utilize local communication and iterative computation. To make our treatment concrete, we considered the problem of computing the average of real-valued input at the nodes in the network. For instance, the real-valued input may be the value of the local clock at each node in the MANET, or data sensed by a local sensor. With these inputs, the nodes need to agree on the average value of the inputs at all the nodes in the network. When transmission losses occur, the traditional iterative algorithms for average consensus fail to reach convergence on the average value. Due to the message losses, the algorithms may often underestimate the average. We developed a novel mechanism to mitigate this shortcoming, by introducing a small amount of additional state at each node. The additional state, in effect, emulates a virtual buffer that holds information, which may otherwise be lost when messages are lost on wireless links. It has been proven that the proposed algorithm can converge to the average despite lossy behavior of the wireless links. The proposed algorithm provides useful insights on how to design iterative algorithms over wireless links.

(2) Improving Throughput of Agreements

The Byzantine model has been used to characterize arbitrary behaviors of an adversary. Thus, the model is useful when an adversary compromises nodes in the network. There has been significant research on agreement in presence of Byzantine nodes. Traditionally, the research on Byzantine agreement focuses on the total message or bit-complexity of achieving an agreement. In our work, we designed algorithms that can achieve optimal throughput of agreement, given the rate region of the underlying network. The throughput of agreement is defined as the long-term average of the number of information bits being agreed upon per unit time. We considered the problem under the constraint that each link in the system has a fixed finite capacity. This contribution is of interest in MANETs wherein a certain capacity on each link is allocated for the purpose of executing the agreement mechanisms. We identified necessary conditions for agreement throughput at rate R bits/unit time to be achievable in general networks. These necessary conditions serve as an upper bound on the agreement capacity. However, whether this bound is tight or not remains an open problem in general. We have developed an algorithm structure that is inspired by the literature on network coding. Following this structure, we designed capacity-achieving algorithms for four-node networks with at most one compromised node and arbitrary link capacity distribution, and also for a class of symmetric networks in which all links have the same capacity. While characterizing the exact Byzantine agreement capacity in general network topologies is still an open problem, we have also developed algorithms that are guaranteed to achieve a constant fraction of the capacity in arbitrary topologies.

We also investigated the communication complexity of agreement. The communication complexity of an algorithm C(L) is defined as the maximum of the total number of bits transmitted by all the nodes according to the algorithm until agreement on L bits is reached correctly, considering all possible misbehaviors of the faulty nodes. This measure of complexity is widely used by the distributed computing community. The per-bit communication complexity of an algorithm is then defined as C(L)/L. We have proposed a deterministic multi-valued algorithm that solves the Byzantine broadcast problem deterministically for L bits in a network with n nodes and at most $t<n/3$ faulty nodes, with C(L) approximately equal to $n(n-1)L/(n-t)$ bits for large L. Hence, for large L, this algorithm achieves per-bit complexity approaching $n(n-1)/(n-t)$, which is linear in n for non-trivial values of t. We are also able to prove that the per-bit complexity of the proposed algorithm is within a constant factor of 2 of optimal. Using ideas introduced in the deterministic multi-valued one-to-many Byzantine broadcast algorithm, we also designed a deterministic multi-valued all-to-all Byzantine consensus algorithm with linear complexity per bit agreed upon.

Related to the problem of agreement, we studied the performance of a probabilistic gossip algorithm in multi-channel wireless networks in the presence of an adversary. We considered a single-hop wireless network composed of n nodes. Each node has kf radios and the wireless spectrum is divided to kC channels, where k is an integer. At the beginning of each time slot, each node chooses kf channels uniformly at random out of kC channels and tunes to them till the end of the time slot. At each time slot, a node decides to transmit on all of its radios with probability p, or receive on all of them with probability 1-p. At each time slot, the adversary chooses kf channels uniformly at random and jams them. Since the network is a single-hop network, if more than one node transmit on the same channel at the same time slot, the messages are corrupted and no useful data can be transferred to the nodes listening on the channel. Via simulations, we investigated the effect of changing k on the termination time of the gossip algorithm. In the gossip algorithm, each node begins the algorithm with an initial value and it attempts to transmit its initial value to the other nodes and receive the initial value of the other nodes. We consider all-to-all gossiping, in which the algorithm terminates whenever every node receives the initial value of all other nodes. We simulated the gossip algorithm for several different values of f and C to determine the optimum k that minimizes the termination time in each case.

(3) Achieving Exact Consensus in Presence of Directed Links

In MANET, due to the asymmetry in interference or channel characteristics, the available communication links may be asymmetric or directed links. When designing algorithms for such networks, one can either ignore the asymmetric links (using only the bidirectional links available), or attempt to exploit the asymmetric links to improve performance. In our work, we have explored strategies to exploit all available network links, including directed or asymmetric links. In particular, we have developed characterization of network graph topologies in which exact consensus is feasible on *discrete* quantities, despite the presence of adversarial (or compromised nodes). Such exact consensus algorithms are necessary to allow the nodes in the MANET to coordinate a common action (e.g., whether to collectively change the transmit power to a higher level or not). Informally, the necessary condition on the underlying graph, to be able to tolerate f compromised nodes, is as follows: if we remove any arbitrary set of f nodes in the network, and partition the rest of the network into sets of nodes L, R and C, then in the resulting graph, either the nodes in L have at least f+1 incoming *external* neighbors, or the nodes in R have at least f+1 incoming *external* neighbors. This condition generalizes on the notion of node connectivity. We show the sufficiency of the necessary condition constructively by developing an algorithm that can correctly solve the exact consensus problem.

By including additional conditions, beyond those necessary for exact consensus, it is also possible to obtain sufficient conditions for achieving broadcast over directed graphs in presence of adversarial nodes. In particular, the additional condition is to require 2f+1 disjoint directed paths from the source of the broadcast to each of the remaining nodes. The additional condition then can be used along with the above condition to allow the source node to transmit its state information to the other nodes in a consistent manner.

(4.4.4) Anonymous Communications in the Presence of Eavesdroppers

(1) A Statistical Framework for Source Anonymity in Sensor Networks

In certain applications, the locations of events reported by a sensor network need to remain anonymous. That is, unauthorized observers must be unable to detect the origin of such events by analyzing the network traffic. Known as the source anonymity problem, this problem has emerged as an important topic in the security of wireless sensor networks, with variety of techniques based on different adversarial assumptions being proposed. In this work, we present a new framework for modeling, analyzing and evaluating anonymity in sensor networks. The novelty of the proposed framework is twofold: first, it introduces the notion of “interval indistinguishability” and provides a

quantitative measure to model anonymity in wireless sensor networks; second, it maps source anonymity to the statistical problem of binary hypothesis testing with nuisance parameters. We then analyze existing solutions for designing anonymous sensor networks using the proposed model. We show how mapping source anonymity to binary hypothesis testing with nuisance parameters leads to converting the problem of exposing private source information into searching for an appropriate data transformation that removes or minimize the effect of the nuisance information. By doing so, we transform the problem from analyzing real-valued sample points to binary codes, which opens the door for coding theory to be incorporated into the study of anonymous sensor networks. Finally, we discuss how existing solutions can be modified to improve their anonymity. Results accepted to appear in IEEE TMC.

(2) Minimizing Anonymous-Communication Vulnerabilities in a Multi-Path Network

In this work, given a multipath wireless network with covert and visible relays, we investigate how to analytically choose routes for each source-destination pair in order to offer maximum anonymity while maintaining a packet-loss constraint. We consider two types of packet-loss: link quality, determined by transmission power and the distance between nodes, and packets dropped by covert relays due to buffer constraints. We formulate the route selection problem within a rate-distortion framework, in which the fraction of flow allocated to each route is chosen to maximize the network anonymity without violating packet-loss constraints. We consider that the network is prefixed with fixed set of regular relays and mix nodes and the adversary can eavesdrop on all links. We then show that the flow allocation to minimize the information leakage to the adversary with packet loss constraints can be formulated as a Rate-Distortion optimization problem. These are preliminary results only. However, even at this early stage, we are able to show that the maximizing anonymity leads to the same optimization problem as capacity finding (Blahut-Arimoto family of algorithms) problem as the original problem is shown to be convex. The result for sources that operate independently was reported in IEEE ISIT 2012. We then consider the case that the sources may have partial information of each other and show that this can also leads to formulation that is mathematically similar to capacity finding algorithms. This is to be presented in the week of October 2012 at the 50th Allerton Conference in Urbana.

An important aspect of our project is the identification of the capabilities an adversary can exercise in attacking basic protocols. By identifying such capabilities, we can design secure protocols that withstand adversary attacks.

(4.4.5) Jamming-Protection Schemes

We developed four schemes that directly counter a jamming adversary. First, we developed a tree-based scheme that uses asymmetric knowledge between a sender and a receiver in order to counter an insider that jams broadcast messages. By sending each broadcast message both on a set of codes called a *cover*, and on a set of *test codes*, the sender can eventually isolate jammers on their own code, minimizing interference to legitimate nodes. Second, we developed a scheme for sleep scheduling that forces an energy-limited jammer to stay awake all the time, quickly depleting its battery power. Next, we developed JIM-Beam, an uncoordinated broadcast anti-jamming mechanism. Unlike prior work in keyless broadcast anti-jamming, JIM-Beam uses spatial diversity rather than frequency- or code-division, which has three major advantages. First, it gives strong security guarantees against a single adversary; second, it prevents wideband jamming because an attacker cannot distribute himself evenly in space; and finally, it allows users to send longer messages because reactive jamming in the spatial domain is much slower than reactive jamming in frequency or code. Finally, we developed SimpleMAC, a MAC protocol that is resilient to MAC-aware attacks. Specifically, SimpleMAC uses a jamming-resilient signaling scheme in place of the traditional control channel, and uses a transmitter strategy to share channel coordination information with a select group of nodes called the *recipient list*. SimpleMAC eventually converges to optimal performance, and almost immediately performs better than the no-MAC Nash equilibrium.

In the area of trusted core, we developed a bottom-up system to ensure epsilon-optimal performance in the long run. We started by using clock synchronization to detect wormhole attackers with equal capability as the normal users, and we expanded our protocol to allow for network-wide clock synchronization. We then developed a routing and scheduling mechanism that ensures epsilon-optimality over a sufficiently-long but bounded period of time. Finally, we extended our algorithm to work even when not all nodes start at the same time; in fact, we can have the network run for an unbounded amount of time before the last node joins, and still achieve epsilon-optimality for a fixed period of time after that node joins.

In vehicular networks, we explored the topic of trust and revocation, designing mechanisms for rapidly disseminating certificate revocation lists and exploring limitations on revocation. Our results show that vehicle mobility can effectively disseminate information over a large scale with little overhead. We have also taken strides in the deployment of VANETs, being the first work to characterize large-scale performance on actual mobility traces, as well as to determine the communications requirements for specific crash-avoidance applications. Our results provide a methodology for evaluating safety application performance requirements, and use intersection collision warning as an example. These results show that safety applications may have very different requirements from traditional data-driven network applications; for example, they may better tolerate losses, since each packet contains relatively little information, but may be much more sensitive to latency. We also developed power control mechanisms for avoiding congestion collapse in rush-hour traffic scenarios, and for limiting the privacy loss due to RF fingerprinting.

We developed a routing protocol, SEAR, for secure routing in ad hoc networks. We developed optimal secure localization schemes, showing the fundamental limits of combining the results of multiple verifiers when faced with a colluding adversary. We secured hybrid networks, ensuring that an attacker must always help the network achieve higher bandwidth with the help of the attacker, as compared to the case where the attacker were absent. We examined false channel condition reports, considering the impact on a variety of protocols when the adversary reports a channel condition either stronger or weaker than the actual condition. Finally, we developed CRAFT, which forces each flow to be TCP-friendly, even under a very weak deployment model, and even when routes are substantially asymmetric.

A significant accomplishment was the completion of the development of a complete clean-slate approach to secure wireless networking that was motivated by and commenced during this contract. There are extensions to be done, but we have completed the development of one complete clean-slate suite of protocols.

(4.4.6) Wiretap and Collaborative Jamming

The inherent openness of wireless communications makes it vulnerable to eavesdropping attacks. Following Shannon’s work on perfect secrecy, the secrecy problem is that of communicating a message through the Bob channel without conveying information about the message through the Eve’s channel. Later Wyner showed that when the Eve’s channel is a degraded version of the legitimate Bob’s channel, a positive information rate between Alice and Bob can be achieved.

The role of multiple antennas in wiretap channels has received much attention recently. For multi-antenna systems, assuming the channel state information is available at Alice, the available degree of freedom can be utilized to substantially degrade Eve’s effective channel. In "Robust beam forming for MISO wiretap channel by optimizing the worst-case secrecy capacity," and "Optimal transmit design for worst-case secrecy rate over uncertain MISO channels," we studied transmit design, without additional jammers’ help. The channel state information (CSI) of Eve and Bob is assumed to

be imperfectly known. Given the uncertainty of the CSI, an optimal transmit covariance is solved to maximize a worst-case secrecy rate under the uncertainty.

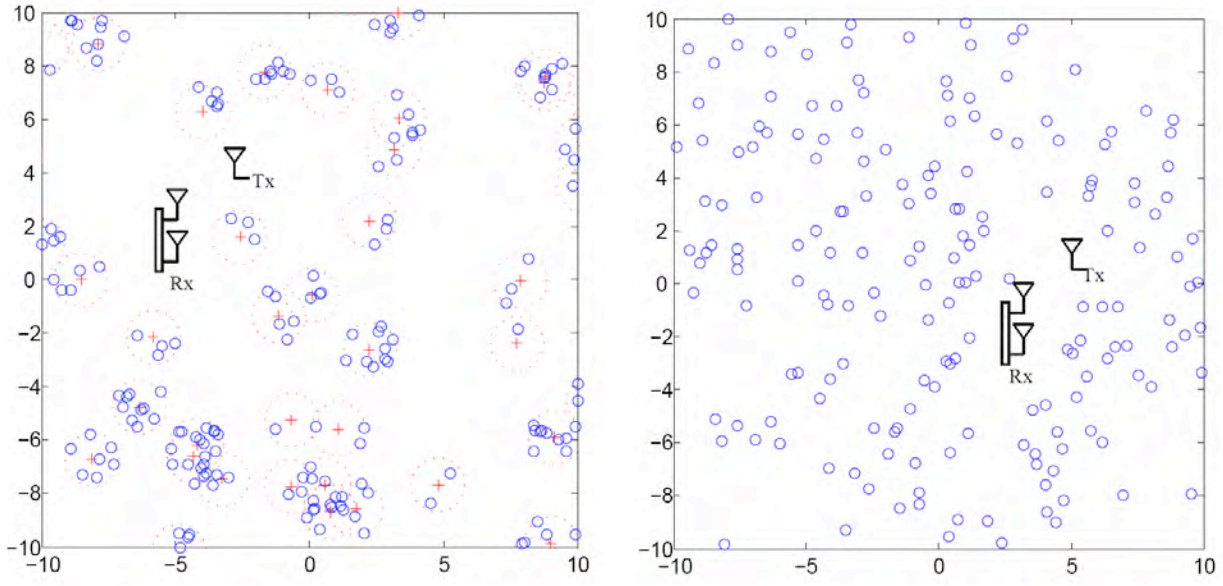
Another idea of utilizing multiple antennas is to interfere Eve through artificial spatial noise, which is referred to as collaborative jamming or friendly jamming. The artificial noise can substantially degrade Eve's channel quality with little or no harm to Bob's channel. Given perfect CSI, found an optimal joint design of transmit/jamming co-variances for MISO (multi-antenna Tx and jammer, single-antenna Rx Eve) wiretap channels (see A. W. Shi and J. Ritcey, "Cooperative transmit and jamming for maximizing secrecy rate of Gaussian MISO wiretap channels," IEEE Trans. Commun.), This was later extended to the case of MISOME (multi-antenna Tx and jammer, single-antenna Rx and multi-antenna Eve) wiretap channel (see J. Ritchey "Transmit beamforming and cooperative jamming for MIMOME wiretap channels," Asilomar Conf. on Signals Systems Computers, pp. 285-289, Nov. 2011). Given imperfect CSI, we proposed a new solution and its effectiveness has been demonstrated by several examples of location uncertainty.

(4.4.7) Interference Analysis for Large Networks

A wireless network can be viewed as a collection of nodes, located in some domain, and can be transmitters or receivers. As wireless networks become more pervasive with denser deployments, interference management has been becoming a defining issue of wireless network design. At a given time, several nodes transmit simultaneously, each toward its own receiver. The signal received from the link transmitter may be jammed by the signals received from the other transmitters. The geometry of the locations of the nodes plays a key role since it determines the signal to interference and noise ratio (SINR) at each receiver.

Stochastic geometry provides a natural way of defining and computing macroscopic properties of such networks, by averaging over all potential geometrical patterns for the nodes. The advantages of using stochastic geometry are: 1) performance metric can be exactly derived in some important cases, and tightly bounded in many others; 2) performance depends on fundamental network parameters, such as the densities of the underlying point processes. Design insights are obtainable from these performance expressions. A software tool is under development that generates and analyzes network interference models based on stochastic geometry.

Our goal is to characterize interference and the performance of multi-antenna receiver in large districted networks. Our work "Performance of MMSE multi-antenna receiver under hierarchical Poisson random fields of interferences," Asilomar Conf. on Signals Systems Computers, Nov. 2012, accepted, and "Performance of MMSE receiver: superposition property of multiple Poisson fields and its application to Poisson clustered interferers," IEEE Trans. Wireless Commun. (in prep) extends the performance analysis of multi-antenna minimum-mean-square-error (MMSE) receivers under Poisson point process (PPP) of interferers to that under more sophisticated Poisson spatial distributions, such as in-homogeneous PPP and Poisson clustered processes. These papers reveal an important fact that the effective interference caused by superposition of PPPs is the sum of the responses which would have been caused by each PPP individually.



(a) (b)

Fig. 1. (a) A realization of the Matern cluster process with parent density $\lambda_p = 0.1$, expected children number $\bar{c} = 5$ and radius $d_c = 5$. Parent point process are homogeneously Poisson distributed with λ_p, and $\bar{c}$ denotes the expected number of children per cluster. The children points are scattered independently identical distribution, around the parent point. Parent points are plotted in red '+' and children in blue 'o' enclosed in dotted circles. (b) A realization of a homogeneous PPP with density $\lambda = 0.5$. Note that the two processes have the same density $\lambda_p = \lambda$.

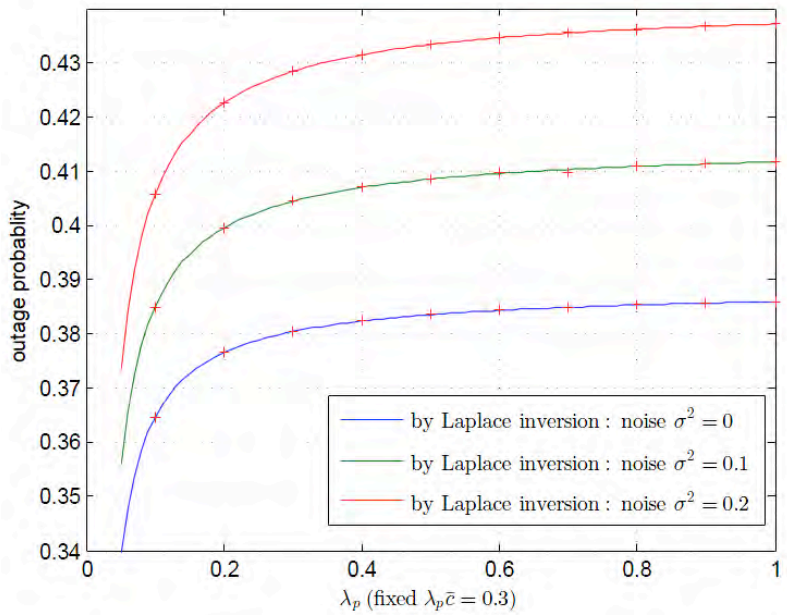


Fig. 2. Comparison of the simulated SINR outage and the theoretic SINR outage. We fix the density $\lambda_p = 0.3$ for better illustration (the resulting outage will vary within a small range). Matern process with $d_c = 1$ is used as the children process. The SINR threshold is set to $\gamma = 0$dB, and antenna number is $L = 3$. The theoretic results are plotted in solid curves, and the simulation results in '+'. The comparison shows that the theoretic calculation is accurate.

Another paper "Distributed jamming for secure communication in a Poisson field of legitimate nodes and eavesdroppers," Asilomar Conf. on Signals Systems Computers, Nov. 2012 (accepted) investigates how cooperative jamming helps improve the secrecy throughput of large decentralized networks where the locations and channel state information (CSI) of eavesdroppers are both

unknown. The spatial distribution of legitimate nodes including transmitter, receiver and helping jammers, and eavesdroppers are modeled as Poisson point process. A jamming protocol based on the RTS/CTS handshake of IEEE 802.11 standard is proposed for decentralized implementation. Our results show that multi-antenna helping jammers can significantly increase the secrecy of the network, compared to single-antenna jammers.

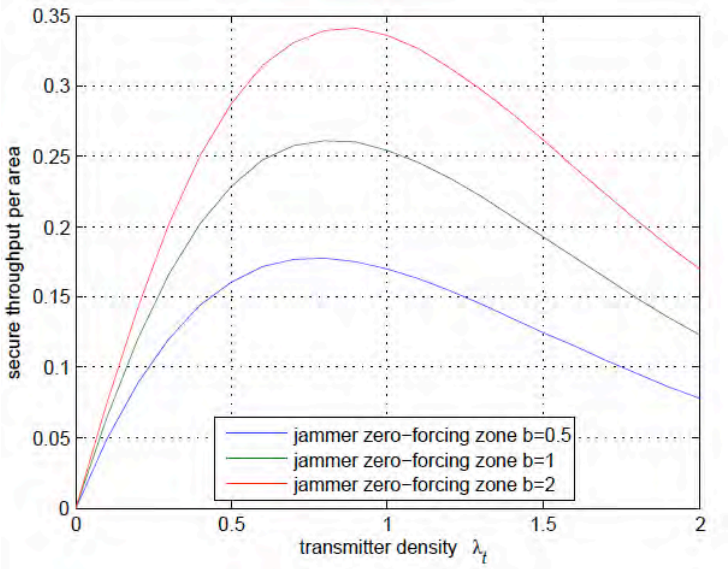


Fig. 3. The secure throughput versus density of legitimate transmitters λ_t. Other network parameters are jammer density $\lambda_j = 1m^{-2}$, eavesdropper density $\lambda_e = 0.2m^{-2}$, transmitter power $P_t = 1$, and jammer power $P_j = 1$. The number of antennas for transmitter and eavesdropper are $N_t = N_e = 2$ respectively.

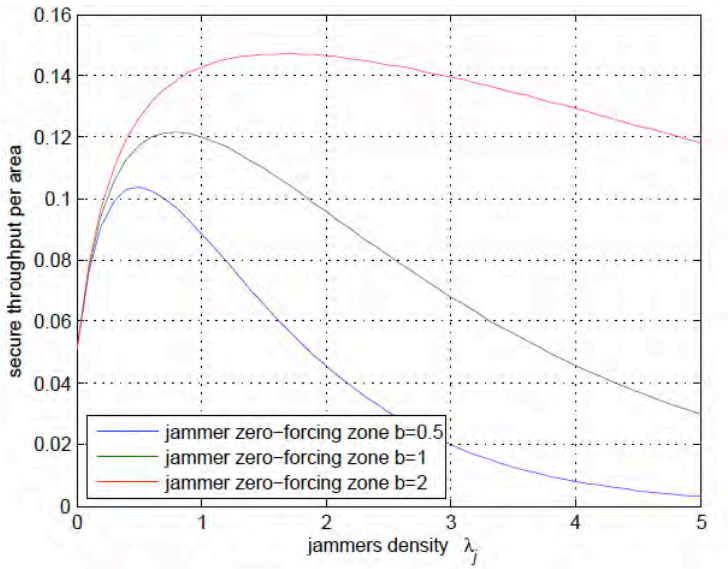


Fig. 4. The secure throughput versus jammer density λ_j. Other network parameters are transmitter density $\lambda_t = 0.1m^{-2}$, eavesdropper density $\lambda_e = 0.2m^{-2}$, transmitter power $P_t = 1$, and jammer power $P_j = 1$. The number of antennas for transmitter and eavesdropper are $N_t = N_e = 2$ respectively.

(4.4.8) Interference Analyzer for a Multi-antenna Wireless Network IA-MWiN

This tool calculates performance metrics of multi-antenna nodes in a decentralized network in visualized manner, where the underlying network nodes are generated by Poisson point process and Poisson clustered processes. These nodes introduce interference into the ad-hoc and clustered ad-hoc network. This augments current methods in which the locations of the network nodes are given,

or deterministic. The node locations are used to compute an interference map and the outage probability, which in term determines the connectivity of nodes.

The tool generates Poisson and Matern clustered nodes. An interference map can be created, conditional on the node locations, and fading model. The outage probability is computed when multi-antenna MMSE received is employed, and the number of antenna elements varied. Network connectivity is determined on anode-to-node basis. The outage results are used to threshold each pairwise link, connecting those in which the outage is below the threshold.

(5) Technology transfer

Collaboration and interaction with RDEC/CERDEC scientists and engineers, Dr. C.J. Graff and Mr. D.G. Yee, on modeling-simulation-validation of mobile ad-hoc networks, through a Phase II SBIR with AIMS, Inc. a small company. The collaboration also included transferring of modeling and simulation software to RDEC/CERDEC. During this reporting period work emphasized scheduling based MAC protocols for MANET, like the USAP protocol.

Collaboration with ARL scientists and engineers, Dr. B. Sadler and P. Yu, on the implications of traffic stochastic models of mobile wireless networks on network security and information assurance. During this period we continued the investigation of detection of wormhole attacks and the implications of various traffic models on attack detection performance.

We initiated research collaboration with Bosch Corporate R&D. Graduate student Shalabh Jain had an internship at Bosch Corporate R&D, where he worked in the area of Wireless Sensor networks security.