REPORT DOCUMENTATION PAGE

Form Approved OMB NO. 0704-0188

1. REPORT DATE (DD-MM-YYYY) 21-01-2016	2. REPORT TYPE Final Report	3. DATES COVERED (From - To) 1-Jun-2007 - 31-Aug-2015

4. TITLE AND SUBTITLE
Final Report: ARSENAL: A Cross Layer Architecture for Secure Resilient Tactical Mobile AdHoc Networks

5a. CONTRACT NUMBER
W911NF-07-1-0318

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER
611103

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

6. AUTHORS
K. Levitt, M. Faloutsos, S. Krishnamurthy, A. L. Swindlehurst, M. Jensen, S. Kasera, J. J. Garcia-Luna-Aceves, G. Cao, P. Krishnamurthy, D. Tipper, T. La Porta, P. Mohapatra, F. Wu

7. PERFORMING ORGANIZATION NAMES AND ADDRESSES
University of California - Davis
Sponsored Programs
1850 Research Park Drive, Suite 300
Davis, CA 95618 -6153

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)
52552-CS-MUR.111

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
Our goal in this project is to develop a cross layer architecture that provides comprehensive security and resilience. Depending on the services desired, our architecture will be able to adaptively provide the right trade-offs between performance, security and fault-resilience. Our strategy for building this architecture is as follows. We will undertake three parallel but inter-coupled tasks geared towards a) performing measurements via real deployments and enhancing our understanding of layer dependencies and vulnerabilities in mobile ad hoc networks; these measurements will be on existing testbeds at

15. SUBJECT TERMS
Cross-layer architecture, physical-layer security, jamming, secure routing

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	15. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON Prasant Mohapatra
a. REPORT UU	b. ABSTRACT UU	c. THIS PAGE UU	UU		19b. TELEPHONE NUMBER 530-754-8380

Report Title

Final Report: ARSENAL: A Cross Layer Architecture for Secure Resilient Tactical Mobile AdHoc Networks

ABSTRACT

Our goal in this project is to develop a cross layer architecture that provides comprehensive security and resilience. Depending on the services desired, our architecture will be able to adaptively provide the right trade-offs between performance, security and fault-resilience. Our strategy for building this architecture is as follows. We will undertake three parallel but inter-coupled tasks geared towards a) performing measurements via real deployments and enhancing our understanding of layer dependencies and vulnerabilities in mobile ad hoc networks; these measurements will be on existing testbeds at various PI institutions, b) building analytical models to characterize the behavioral nuances of these networks and c) design of new cross layer protocols that protect against vulnerabilities and provide the desired robustness as mentioned above. The distinguishing aspects of this proposed work are that our approach (i) provides accurate, experimentally validated physical and higher layer characterization and dependencies between layers, (ii) unlike previous approaches, accounts for physical layer effects and exploits specialized physical layer features to provide better security and (iii) models and addresses a comprehensive set of possible attacks including attacks by insider nodes. We have a very strong team of PIs that have expertise in physical layer design and modeling, experimental networking research, protocol design and analysis, fault-tolerance and in security. Some of the PIs have prior records of both success in DoD programs and in working together on joint projects.

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
05/07/2012	27.00	Rolando Menchaca-Mendez, J.J. Garcia-Luna-Aceves. Hydra: Efficient multicast routing in MANETs using sender-initiated multicast meshes, Pervasive and Mobile Computing, (02 2010): 0. doi: 10.1016/j.pmcj.2009.07.010
05/09/2012	4.00	Qinghua Li, Wei Gao, Sencun Zhu, Guohong Cao. A routing protocol for socially selfish delay tolerant networks, Ad Hoc Networks, (07 2011): 0. doi: 10.1016/j.adhoc.2011.07.007
05/09/2012	25.00	Sencun Zhu, Wensheng Zhang, Guohong Cao, Yi Yang, Min Shao. pDCS: Security and Privacy Support for Data-Centric Sensor Networks, IEEE Transactions on Mobile Computing, (08 2009): 0. doi: 10.1109/TMC.2008.168
10/31/2011	2.00	Thaier Hayajneh, Prashant Krishnamurthy, David Tipper, Anh Le. Secure Neighborhood Creation in Wireless Ad Hoc Networks using Hop Count Discrepancies, Mobile Networks and Applications, (7 2011): 0. doi: 10.1007/s11036-011-0334-2
10/31/2011	33.00	J. J. Garcia-Luna-Aceves, Rolando Menchaca-Mendez. PRIME: An Interest-Driven Approach to Integrated Unicast and Multicast Routing in MANETs, IEEE/ACM Transactions on Networking, (01 2011): 0. doi: 10.1109/TNET.2011.2119402
10/31/2011	32.00	Stephen Dabideen, J. J. Garcia-Luna-Aceves. Efficient routing in MANETs using ordered walks, Wireless Networks, (4 2011): 0. doi: 10.1007/s11276-011-0339-6
10/31/2011	31.00	Neal Patwari, Sneha K. Kasera. Temporal Link Signature Measurements for Location Distinction, IEEE Transactions on Mobile Computing, (03 2011): 0. doi: 10.1109/TMC.2010.189
10/31/2011	3.00	Xuan Jiang, Wenhui Hu, Sencun Zhu, Guohong Cao. Compromise-resilient anti-jamming communication in wireless sensor networks, Wireless Networks, (6 2011): 0. doi: 10.1007/s11276-011-0361-8
10/31/2011	6.00	Raju Kumar, Thomas La Porta. Cooperative Channelization in Wireless Networks with Network Coding, IEEE Transactions on Parallel and Distributed Systems, (07 2011): 0. doi: 10.1109/TPDS.2010.175
10/31/2011	7.00	Konstantinos Pelechrinis, Ioannis Broustis, Srikanth V. Krishnamurthy, Christos Gkantsidis. A Measurement-Driven Anti-Jamming System for 802.11 Networks, IEEE/ACM Transactions on Networking, (08 2011): 0. doi: 10.1109/TNET.2011.2106139
10/31/2011	8.00	Konstantinos Pelechrinis, Guanhua Yan, Stephan Eidenbenz, Srikanth V. Krishnamurthy. Detection of Selfish Manipulation of Carrier Sensing in 802.11 Networks, IEEE Transactions on Mobile Computing, (01 2011): 0. doi: 10.1109/TMC.2011.131
10/31/2011	9.00	Konstantinos Pelechrinis, Christos Koufogiannakis, Srikanth V. Krishnamurthy. On the Efficacy of Frequency Hopping in Coping with Jamming Attacks in 802.11 Networks, IEEE Transactions on Wireless Communications, (10 2010): 0. doi: 10.1109/TWC.2010.082310.100113
10/31/2011	10.00	Ioannis Broustis, Konstantinos Pelechrinis, Dimitris Syrivelis, Srikanth V. Krishnamurthy, Leandros Tassiulas. A software framework for alleviating the effects of MAC-aware jamming attacks in wireless access networks, Wireless Networks, (7 2011): 0. doi: 10.1007/s11276-011-0363-6

10/31/2011 11.00 Konstantinos Pelechrinis, Marios Iliofotou, Srikanth V. Krishnamurthy. Denial of Service Attacks in Wireless Networks: The Case of Jammers,
IEEE Communications Surveys & Tutorials, (04 2011): 0. doi: 10.1109/SURV.2011.041110.00022

10/31/2011 12.00 Amitav Mukherjee, A. Lee Swindlehurst. Robust Beamforming for Security in MIMO Wiretap Channels With Imperfect CSI,
IEEE Transactions on Signal Processing, (01 2011): 0. doi: 10.1109/TSP.2010.2078810

10/31/2011 13.00 S. Ali A. Fakoorian, A. Lee Swindlehurst. MIMO Interference Channel With Confidential Messages: Achievable Secrecy Rates and Precoder Design,
IEEE Transactions on Information Forensics and Security, (09 2011): 0. doi: 10.1109/TIFS.2011.2156788

10/31/2011 14.00 S. Ali A. Fakoorian, A. Lee Swindlehurst. Solutions for the MIMO Gaussian Wiretap Channel With a Cooperative Jammer,
IEEE Transactions on Signal Processing, (10 2011): 0. doi: 10.1109/TSP.2011.2161298

10/31/2011 17.00 Daniel N Evans, Michael A Jensen. Near-Optimal Radiation Patterns for Antenna Diversity,
IEEE Transactions on Antennas and Propagation, (11 2010): 0. doi: 10.1109/TAP.2010.2071338

10/31/2011 16.00 Michael A. Jensen, Chan Chen. Secret Key Establishment Using Temporally and Spatially Correlated Wireless Channel Coefficients,
IEEE Transactions on Mobile Computing, (02 2011): 0. doi: 10.1109/TMC.2010.114

10/31/2011 15.00 Michael A. Jensen, Yan Shi. Feedback Reduction for CDI-Based Beamforming in the MIMO Broadcast Channel,
IEEE Communications Letters, (04 2011): 0. doi: 10.1109/LCOMM.2011.030911.101861

10/31/2011 18.00 Michael A. Jensen, Buon Kiong Lau. Uncoupled Matching for Active and Passive Impedances of Coupled Arrays in MIMO Systems,
IEEE Transactions on Antennas and Propagation, (10 2010): 0. doi: 10.1109/TAP.2010.2055803

11/04/2011 20.00 B.T. Quist, M.A. Jensen. Optimal Antenna Radiation Characteristics for Diversity and MIMO Systems,
IEEE Transactions on Antennas and Propagation, (11 2009): 0. doi: 10.1109/TAP.2009.2026922

11/04/2011 21.00 M.A. Jensen, J.W. Wallace. Sparse Power Angle Spectrum Estimation,
IEEE Transactions on Antennas and Propagation, (08 2009): 0. doi: 10.1109/TAP.2009.2024465

11/04/2011 22.00 N. Patwari, J. Croft, S. Jana, S.K. Kasera. High-Rate Uncorrelated Bit Extraction for Shared Secret Key Generation from Channel Measurements,
IEEE Transactions on Mobile Computing, (01 2010): 0. doi: 10.1109/TMC.2009.88

11/04/2011 23.00 S.K. Kasera, S. Jana. On Fast and Accurate Detection of Unauthorized Wireless Access Points Using Clock Skews,
IEEE Transactions on Mobile Computing, (03 2010): 0. doi: 10.1109/TMC.2009.145

11/04/2011 24.00 Thaier Hayajneh, Razvi Doomun, Prashant Krishnamurthy, David Tipper. Source-destination obfuscation in wireless ad hocnetworks,
Security and Communication Networks, (08 2011): 0. doi: 10.1002/sec.220

11/04/2011 26.00 Stephen Dabideen, Bradley R. Smith, J. J. Garcia-Luna-Aceves. An end-to-end approach to secure routing in MANETs,
Security and Communication Networks, (03 2010): 0. doi: 10.1002/sec.121

11/04/2011 88.00 Prantik Bhattacharyya, Ankush Garg, Shyhtsun Felix Wu. Analysis of user keyword similarity in online social networks,
Social Network Analysis and Mining, (10 2010): 0. doi: 10.1007/s13278-010-0006-4

11/04/2011 95.00 Kai Zeng, Kannan Govindan, Prasant Mohapatra. Non-cryptographic authentication and identification in wireless networks [Security and Privacy in Emerging Wireless Networks,
IEEE Wireless Communications, (10 2010): 0. doi: 10.1109/MWC.2010.5601959

11/04/2011 96.00 Dhruv Gupta, Daniel Wu, Prasant Mohapatra, Chen-Nee Chuah. A study of overheads and accuracy for efficient monitoring of wireless mesh networks,
Pervasive and Mobile Computing, (02 2010): 0. doi: 10.1016/j.pmcj.2009.07.011

TOTAL: **30**

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

Number of Presentations: 0.00

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

Received Paper

11/04/2011 97.00 Mass, D., Patwari, N., Zhang, J., Kasera, K. Sneha, Jensen. M. Location distinction in a MIMO channel,
Virginia Tech Symposium on Wireless Personal Communications, June 2009. , . : ,

11/04/2011 98.00 Hayajneh, T., Krishnamurthy, P., Tipper, D.. secund: a Protocol for SECUre NeighborhooD Creation in Wireless Ad hoc Networks,
CollaborateCom '09, Washington DC, November 2009. , . : ,

11/04/2011 99.00 Jiang, X, Hu, W, Zhu, S, Cao, G. Compromise-Resilient Anti-Jamming for Wireless Sensor Networks,
Twelfth International Conference on Information and Communications Security, 2010. , . : ,

TOTAL: **3**

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

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

Received		Paper
05/07/2012	54.00	Liang Cai, Kai Zeng , Hao Chen , Prasant Mohapatra. Good Neighbor: Ad Hoc Pairing Of Nearby Wireless Devices By Multiple Antennas, Proceedings of the Network and Distributed System Security Symposium, NDSS 2011. 09-FEB-11, . : ,
05/09/2012	75.00	Konstantinos Pelechrinis, Ioannis Broustis, Srikanth V. Krishnamurthy, Christos Gkantsidis. ARES: An Anti-Jamming Re-Inforcement System, the 5th international conference. 30-NOV-09, Rome, Italy. : ,
10/31/2011	1.00	Yunchuan Wei, Kai Zeng, Prasant Mohapatra. Adaptive wireless channel probing for shared key generation, IEEE INFOCOM 2011 - IEEE Conference on Computer Communications. 09-APR-11, Shanghai, China. : ,
10/31/2011	5.00	Zhichao Zhu, Guohong Cao. APPLAUS: A Privacy-Preserving Location Proof Updating System for location-based services, IEEE INFOCOM 2011 - IEEE Conference on Computer Communications. 09-APR-11, Shanghai, China. : ,
10/31/2011	19.00	Yan Shi, M. A. Jensen. Identifying MIMO wireless devices based on radiometric signatures, 2011 IEEE Antennas and Propagation Society International Symposium and USNC/URSI National Radio Science Meeting. 02-JUL-11, Spokane, WA. : ,
10/31/2011	28.00	Yan Shi, , Jensen, M.A.. Scheduling multi-user MIMO communication based on physical channel parameters, Antennas and Propagation (EUCAP), Proceedings of the 5th European Conference on . 11-APR-11, . : ,
10/31/2011	29.00	Jensen, M.A., , Buon Kiong Lau, , Medbo, J., , Furuskog, J.. Performance of cooperative MIMO based on measured urban channel data, Antennas and Propagation (EUCAP), Proceedings of the 5th European Conference on . 11-APR-11, . : ,
10/31/2011	30.00	Yan Shi, Michael A. Jensen. Efficient Link Scheduling for MIMO Ad Hoc Networks in Time-Varying Channels, GLOBECOM 2010 - 2010 IEEE Global Communications Conference. 05-DEC-10, Miami, FL, USA. : ,
11/01/2011	35.00	Kunjie Xu, Siriluck Tipmongkonsilp, David Tipper, Prashant Krishnamurthy, Yi Qian. A time dependent performance model for multihop wireless networks with CBR traffic, 2010 29th IEEE International Performance Computing and Communications Conference (IPCCC). 09-DEC-10, Albuquerque, NM, USA. : ,
11/01/2011	57.00	Rumi Ghosh, J.J. Garcia-Luna-Aceves, Rolando Menchaca-Mendez. An interest-driven approach for unicast routing in MANETs with labeled paths and proactive path maintenance, 2011 IEEE Wireless Communications and Networking Conference (WCNC). 27-MAR-11, Cancun, Mexico. : ,
11/01/2011	56.00	J.J. Garcia-Luna-Aceves, Rolando Menchaca-Mendez. A cross-layer framework to support real-time and elastic traffic in MANETs, 2011 IEEE Wireless Communications and Networking Conference (WCNC). 27-MAR-11, Cancun, Mexico. : ,

11/01/2011 55.00 Junxing Zhang, Sneha K. Kasera, Neal Patwari, Piyush Rai. Distinguishing locations across perimeters using wireless link measurements,
IEEE INFOCOM 2011 - IEEE Conference on Computer Communications. 09-APR-11, Shanghai, China. : ,

11/01/2011 53.00 Kai Zeng, Kannan Govindan, Daniel Wu, Prasant Mohapatra. Identity-based attack detection in mobile wireless networks,
IEEE INFOCOM 2011 - IEEE Conference on Computer Communications. 09-APR-11, Shanghai, China. : ,

11/01/2011 52.00 Xinjie Yang, A. Lee Swindlehurst. On the use of artificial interference for secrecy with imperfect CSI,
2011 IEEE 12th Workshop on Signal Processing Advances in Wireless Communications (SPAWC 2011). 25-JUN-11, San Francisco, CA, USA. : ,

11/01/2011 51.00 S. Ali A. Fakoorian, A. Lee Swindlehurst. Secrecy capacity of MISO Gaussian wiretap channel with a cooperative jammer,
2011 IEEE 12th Workshop on Signal Processing Advances in Wireless Communications (SPAWC 2011). 25-JUN-11, San Francisco, CA, USA. : ,

11/01/2011 50.00 Jing Huang, A. Lee Swindlehurst. Cooperation strategies for secrecy in MIMO relay networks with unknown eavesdropper CSI,
ICASSP 2011 - 2011 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP). 21-MAY-11, Prague, Czech Republic. : ,

11/01/2011 49.00 Jing Huang, A. Swindlehurst. Secure Communications via Cooperative Jamming in Two-Hop Relay Systems,
GLOBECOM 2010 - 2010 IEEE Global Communications Conference. 05-DEC-10, Miami, FL, USA. : ,

11/01/2011 48.00 Amitav Mukherjee, A. Lee Swindlehurst. Optimal strategies for countering dual-threat jamming/eavesdropping-capable adversaries in MIMO channels,
MILCOM 2010 - 2010 IEEE Military Communications Conference. 30-OCT-10, San Jose, CA, USA. : ,

11/01/2011 47.00 S. Ali. A. Fakoorian, A. Lee Swindlehurst. MIMO interference channel with confidential messages: Game theoretic beamforming designs,
2010 44th Asilomar Conference on Signals, Systems and Computers. 06-NOV-10, Pacific Grove, CA, USA. : ,

11/01/2011 46.00 A. Mukherjee, A. L. Swindlehurst. Ensuring Secrecy in MIMO Wiretap Channels with Imperfect CSIT: A Beamforming Approach,
ICC 2010 - 2010 IEEE International Conference on Communications. 22-MAY-10, Cape Town, South Africa. : ,

11/01/2011 45.00 A. Mukherjee, A. L. Swindlehurst. Equilibrium Outcomes of Dynamic Games in MIMO Channels with Active Eavesdroppers,
ICC 2010 - 2010 IEEE International Conference on Communications. 22-MAY-10, Cape Town, South Africa. : ,

11/01/2011 44.00 A. Lee Swindlehurst, Amitav Mukherjee. Poisoned feedback: The impact of malicious users in closed-loop multiuser mimo systems,
2010 IEEE International Conference on Acoustics, Speech and Signal Processing. 13-MAR-10, Dallas, TX, USA. : ,

11/01/2011 43.00 Mustafa Y. Arslan, Jongwon Yoon, Karthikeyan Sundaresan, Srikanth V. Krishnamurthy, Suman Banerjee. FERMI a femtocell resource management system forinterference mitigation in OFDMA ,
the 17th annual international conference. 19-SEP-11, Las Vegas, Nevada, USA. : ,

11/01/2011 42.00 Zi Feng, Jianxia Ning, Ioannis Broustis, Konstantinos Pelechrinis, Srikanth V. Krishnamurthy, Michalis Faloutsos. Coping with packet replay attacks in wireless networks,
2011 8th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON). 27-JUN-11, Salt Lake City, UT, USA. : ,

11/01/2011 36.00 Aylin Aksu, Prashant Krishnamurthy. Sub-area localization: a simple calibration free approach, the 13th ACM international conference. 16-OCT-10, Bodrum, Turkey. : ,

11/01/2011 37.00 A. Aksu, P. Krishnamurthy, D. Tipper, O. Ercetin. On security and reliability using cooperative transmissions in sensor networks,
Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom), 2010 6th International Conference on . 09-OCT-10, . : ,

11/01/2011 38.00 Qinghua Li, Sencun Zhu, Guohong Cao. Routing in Socially Selfish Delay Tolerant Networks,
IEEE INFOCOM 2010 - IEEE Conference on Computer Communications. 14-MAR-10, San Diego, CA, USA. : ,

11/01/2011 34.00 Tae-Hoon Kim, David Tipper, Prashant Krishnamurthy. Improving the Connectivity of Heterogeneous Multi-Hop Wireless Networks,
ICC 2011 - 2011 IEEE International Conference on Communications. 05-JUN-11, Kyoto, Japan. : ,

11/01/2011 39.00 Raju Kumar, Srikar Tati, Felipe de Mello, Srikanth V. Krishnamurthy, Thomas La Porta. Network Coding aware Rate Selection in multi-rate IEEE 802.11,
2010 18th IEEE International Conference on Network Protocols (ICNP). 05-OCT-10, Kyoto, Japan. : ,

11/01/2011 40.00 Raju Kumar, Sharanya Eswaran, Thomas La Porta. End-to-end rate selection for opportunistic reception in multi-rate wireless networks,
2011 8th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON). 27-JUN-11, Salt Lake City, UT, USA. : ,

11/04/2011 41.00 Ece Gelal, Konstantinos Pelechrinis, Ioannis Broustis, Srikanth V. Krishnamurhty, Saif Mohammed, A. Chockalingam, Sneha Kasera. On the Impact of MIMO Diversity on Higher Layer Performance,
2010 IEEE 30th International Conference on Distributed Computing Systems. 21-JUN-10, Genoa, Italy. : ,

11/04/2011 58.00 Yanling Yang, Michael A. Jensen. MIMO channel spatial covariance estimation: Analysis using a closed-form model,
2010 IEEE International Conference on Wireless Information Technology and Systems (ICWITS). 28-AUG-10, Honolulu, HI, USA. : ,

11/04/2011 59.00 Chan Chen, Michael A. Jensen. Improved channel quantization for secret key establishment in wireless systems,
2010 IEEE International Conference on Wireless Information Technology and Systems (ICWITS). 28-AUG-10, Honolulu, HI, USA. : ,

11/04/2011 60.00 Michael A. Jensen, Chan Chen. Encryption key establishment using space-time correlated MIMO channels,
2010 IEEE International Symposium Antennas and Propagation and CNC/USNC/URSI Radio Science Meeting. 11-JUL-10, Toronto, ON, Canada. : ,

11/04/2011 61.00 Michael A. Jensen, Chan Chen. Secrecy Extraction from Increased Randomness in a Time-Variant MIMO Channel,
GLOBECOM 2009 - 2009 IEEE Global Telecommunications Conference. 30-NOV-09, Honolulu, Hawaii. : ,

11/04/2011 63.00 Sneha K. Kasera, Neal Patwari, Junxing Zhang. Mobility -assisted Secret Key Generation Using Wireless Link Signatures,
IEEE INFOCOM 2010 - IEEE Conference on Computer Communications. 14-MAR-10, San Diego, CA, USA. : ,

11/04/2011 62.00 Srikanth V. Krishnamurthy, Sriram Nandha Premnath, Mike Clark, Sneha K. Kasera, Neal Patwari, Suman Jana. On the effectiveness of secret key extraction from wireless signal strength in real environments,
the 15th annual international conference. 20-SEP-09, Beijing, China. : ,

11/04/2011 64.00 Jessica Croft, Neal Patwari, Sneha K. Kasera. Robust uncorrelated bit extraction methodologies for wireless sensors,
the 9th ACM/IEEE International Conference. 12-APR-10, Stockholm, Sweden. : ,

11/04/2011 65.00 Konstantinos Pelechrinis, Ioannis Broustis, Srikanth V. Krishnamurhty, Saif Mohammed, A. Chockalingam, Sneha Kasera, Ece Gelal. On the Impact of MIMO Diversity on Higher Layer Performance,
2010 IEEE 30th International Conference on Distributed Computing Systems. 20-JUN-10, Genoa, Italy. : ,

11/04/2011 66.00 Tae-Hoon Kim, David Tipper, Prashant Krishnamurthy, A. Lee Swindlehurst. Improving the topological resilience of mobile ad hoc networks,
2009 7th International Workshop on Design of Reliable Communication Networks (DRCN). 24-OCT-09, Washington, DC, USA. : ,

11/04/2011 67.00 Thaier Hayajneh, Prashant Krishnamurthy, David Tipper. DeWorm: A Simple Protocol to Detect Wormhole Attacks in Wireless Ad Hoc Networks,
2009 Third International Conference on Network and System Security. 18-OCT-09, Gold Coast, Queensland, Australia. : ,

11/04/2011 68.00 Korporn Panyim, Thaier Hayajneh, Prashant Krishnamurthy, David Tipper. On limited-range strategic/random jamming attacks in wireless ad hoc networks,
2009 IEEE 34th Conference on Local Computer Networks (LCN 2009). 19-OCT-09, Zurich, Switzerland. : ,

11/04/2011 69.00 Razvi Doomun, Thaier Hayajneh, Prashant Krishnamurthy, David Tipper. SECLOUD: Source and Destination Seclusion Using Clouds for wireless ad hoc networks,
2009 IEEE Symposium on Computers and Communications (ISCC). 04-JUL-09, Sousse, Tunisia. : ,

11/04/2011 70.00 Min Shao, Wenhui Hu, Sencun Zhu, Guohong Cao, Srikanth Krishnamurth, Tom La Porta. Cross-layer Enhanced Source Location Privacy in Sensor Networks,
2009 6th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks. 21-JUN-09, Rome, Italy. : ,

11/04/2011 71.00 Sencun Zhu, Qinghua Li, Guohong Cao. Routing in Socially Selfish Delay Tolerant Networks,
IEEE INFOCOM 2010 - IEEE Conference on Computer Communications. 13-MAR-10, San Diego, CA, USA. : ,

11/04/2011 72.00 Tae-Suk Kim, Serdar Vural, Ioannis Broustis, Dimitris Syrivelis, Srikanth V. Krishnamurthy, Thomas F. La Porta. A Framework for Joint Network Coding and Transmission Rate Control in Wireless Networks,
IEEE INFOCOM 2010 - IEEE Conference on Computer Communications. 13-MAR-10, San Diego, CA, USA. : ,

11/04/2011 73.00 Stephen Dabideen, J. J. Garcia-Luna-Aceves. Ordering in time: A new routing approach for wireless networks,
2010 IEEE 7th International Conference on Mobile Ad-Hoc and Sensor Systems (MASS). 07-NOV-10, San Francisco, CA, USA. : ,

11/04/2011 74.00 Rolando Menchaca-Mendez, J. J. Garcia-Luna-Aceves. Robust and Scalable Integrated Routing in MANETs Using Context-Aware Ordered Meshes,
IEEE INFOCOM 2010 - IEEE Conference on Computer Communications. 13-MAR-10, San Diego, CA, USA. : ,

11/04/2011 76.00 Raju Kumar, Srikar Tati, Felipe de Mello, Srikanth V. Krishnamurthy, Thomas La Porta. Network Coding aware Rate Selection in multi-rate IEEE 802.11,
2010 18th IEEE International Conference on Network Protocols (ICNP). 04-OCT-10, Kyoto, Japan. : ,

11/04/2011 77.00 Amitav Mukherjee, A. Lee Swindlehurst. Utility of beamforming strategies for secrecy in multiuser MIMO wiretap channels,
2009 47th Annual Allerton Conference on Communication, Control, and Computing (Allerton). 29-SEP-09, Monticello, IL, USA. : ,

11/04/2011 78.00 Amitav Mukherjee, A. Lee Swindlehurst. User selection in multiuser MIMO systems with secrecy considerations,
2009 Conference Record of the Forty-Third Asilomar Conference on Signals, Systems and Computers. 31-OCT-09, Pacific Grove, CA, USA. : ,

11/04/2011 79.00 Jianqi Wang, A. Lee Swindlehurst. Cooperative Jamming in MIMO ad-hoc networks,
2009 Conference Record of the Forty-Third Asilomar Conference on Signals, Systems and Computers. 31-OCT-09, Pacific Grove, CA, USA. : ,

11/04/2011 80.00 Amitav Mukherjee, A. Lee Swindlehurst. Poisoned feedback: The impact of malicious users in closed-loop multiuser mimo systems,
2010 IEEE International Conference on Acoustics, Speech and Signal Processing. 13-MAR-10, Dallas, TX, USA. : ,

11/04/2011 81.00 A. Mukherjee, A. L. Swindlehurst. Equilibrium Outcomes of Dynamic Games in MIMO Channels with Active Eavesdroppers,
ICC 2010 - 2010 IEEE International Conference on Communications. 22-MAY-10, Cape Town, South Africa. : ,

11/04/2011 82.00 A. Mukherjee, A. L. Swindlehurst. Ensuring Secrecy in MIMO Wiretap Channels with Imperfect CSIT: A Beamforming Approach,
ICC 2010 - 2010 IEEE International Conference on Communications. 22-MAY-10, Cape Town, South Africa. : ,

11/04/2011 83.00 Amitav Mukherjee, A. Lee Swindlehurst. Securing multi-antenna two-way relay channels with analog network coding against eavesdroppers,
2010 IEEE 11th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC 2010). 20-JUN-10, Marrakech, Morocco. : ,

11/04/2011 84.00 Amitav Mukherjee, A. Lee Swindlehurst. Optimal strategies for countering dual-threat jamming/eavesdropping-capable adversaries in MIMO channels,
MILCOM 2010 - 2010 IEEE Military Communications Conference. 31-OCT-10, San Jose, CA, USA. : ,

11/04/2011 85.00 S. Ali. A. Fakoorian, A. Lee Swindlehurst. MIMO interference channel with confidential messages: Game theoretic beamforming designs,
2010 44th Asilomar Conference on Signals, Systems and Computers. 07-NOV-10, Pacific Grove, CA, USA. : ,

11/04/2011 86.00 Jing Huang, A. Swindlehurst. Secure Communications via Cooperative Jamming in Two-Hop Relay Systems,
GLOBECOM 2010 - 2010 IEEE Global Communications Conference. 06-DEC-10, Miami, FL, USA. : ,

11/04/2011 87.00 Shaozhi Ye, Felix Wu. Estimating the Size of Online Social Networks,
2010 IEEE Second International Conference on Social Computing (SocialCom). 20-AUG-10, Minneapolis, MN, USA. : ,

11/04/2011 89.00 Shaozhi Ye, Juan Lang, Felix Wu. Crawling Online Social Graphs,
2010 12th Asia Pacific Web Conference (APWEB). 06-APR-10, Busan, Korea (South). : ,

11/04/2011 90.00 Daniela Alvim Seabra de Oliveira, S. Felix Wu. Protecting Kernel Code and Data with a Virtualization-Aware Collaborative Operating System,
2009 Annual Computer Security Applications Conference (ACSAC). 06-DEC-09, Honolulu, Hawaii, USA. : ,

11/04/2011 91.00 D. Gupta, P. Mohapatra, C.-N. Chuah. Diagnosing Failures in Wireless Networks Using Fault Signatures,
ICC 2010 - 2010 IEEE International Conference on Communications. 22-MAY-10, Cape Town, South Africa. : ,

11/04/2011 92.00 S. Chen, K. Zeng, P. Mohapatra. Jamming-Resistant Communication: Channel Surfing without Negotiation,
ICC 2010 - 2010 IEEE International Conference on Communications. 22-MAY-10, Cape Town, South Africa. : ,

11/04/2011 93.00 Daniel Wu, Prasant Mohapatra. QuRiNet: A wide-area wireless mesh testbed for research and experimental evaluations,
2010 Second International Conference on COMmunication Systems and NETworks (COMSNETS 2010). 04-JAN-10, Bangalore, India. : ,

11/04/2011 94.00 Kai Zeng, Daniel Wu, An Chan, Prasant Mohapatra. Exploiting Multiple-Antenna Diversity for Shared Secret Key Generation in Wireless Networks,
IEEE INFOCOM 2010 - IEEE Conference on Computer Communications. 13-MAR-10, San Diego, CA, USA. : ,

TOTAL: **66**

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

(d) Manuscripts

Received Paper

TOTAL:

Number of Manuscripts:

Books

Received Book

TOTAL:

Received	Book Chapter

TOTAL:

Patents Submitted

Patents Awarded

Awards

IEEE Fellow: P. Mohapatra, S. Krishnamurthy, M. Jensen, L. Swindlehurst, G. Cao

ACM Fellow: J. J. Garcia-Luna-Aceves

Graduate Students

NAME	PERCENT_SUPPORTED	Discipline
D. Mass	0.25	
P. Gowda	0.25	
X. Cheng	0.50	
K. Tan	0.50	
A. Banerjee	0.50	
H. Bhatia	0.50	
P. Lundrigan	0.50	
M. Khaledi	0.50	
B. Quist	0.50	
F. Sharifabad	0.50	
Q. Li	0.50	
M. Lin	0.50	
A. Fakoorian	0.50	
J. Huang	0.50	
A. Mukherjee	0.50	
Y. Shi	0.50	
D. Evans	0.50	
T. Hayajneh	0.50	
T. H. Kim	0.50	
J. C. Park	0.50	
J. Zhang	0.50	
T. Bolbrock	0.50	
M. Shao	0.50	
W. Wu	0.50	
X. Yang	0.50	
K. Pelechrinis	0.50	
M. Arslan	0.50	
Z. Feng	0.50	
D. Wu	0.50	
D. Gupta	0.50	
H. Yu	0.50	
A. Chan	0.50	
L. Banks	0.50	
M. Spear	0.50	
S. Dabideen	0.50	
J. Zhao	0.50	
M. Shao	0.50	
J. Eriksson	0.50	
D. DeFigueiredo	0.50	
C. Chen	0.50	
Y. Yang	0.50	
K. Xu	0.50	
Q. Li	0.50	
X. Jiang	0.50	
R. Kumar	0.50	
New Entry	0.00	
A. Le	0.50	
S. Singh	0.50	
FTE Equivalent:	**23.00**	
Total Number:	**48**	

Names of Post Doctorates

NAME	PERCENT_SUPPORTED
P. Djukic	0.50
O. Turkcu	0.50
K. Zeng	0.50
G. Papageorgiou	0.50
FTE Equivalent:	**2.00**
Total Number:	**4**

Names of Faculty Supported

NAME	PERCENT_SUPPORTED	National Academy Member
P. Mohapatra	0.20	
K. Levitt	0.10	
S. Krishnamurthy	0.10	
M. Faloutsos	0.10	
P. Krsihnamurthy	0.10	
D. Tipper	0.10	
T. LaPorta	0.10	
G. Cao	0.10	
S. Kasera	0.10	
F. Wu	0.10	
L. Swindlehurst	0.10	
M. Jensen	0.10	
FTE Equivalent:	**1.30**	
Total Number:	**12**	

Names of Under Graduate students supported

NAME	PERCENT_SUPPORTED	Discipline
D. Schukin	0.25	
FTE Equivalent:	**0.25**	
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: 1.00

The number of undergraduates funded by this agreement who graduated during this period with a degree in science, mathematics, engineering, or technology fields:...... 1.00

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:...... 4.00

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 1.00

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
Y. Yang
S. Jana
X. Jiang
M. Clark

Total Number: **4**

Names of personnel receiving PHDs

NAME
J. Zhao
M. Shao
J. Eriksson
D. Defigueriredo
C. Chen
T. Hayajneh
C. Liu
Y. Zhang
K. Pelechrinis
T. H. Kim
Y. Shi
J. Zhang
S. Dabideen

Total Number: **13**

Names of other research staff

NAME	PERCENT_SUPPORTED

FTE Equivalent:
Total Number:

Sub Contractors (DD882)

1 a. University of California - Riverside

1 b. 200 University Office Building

Riverside CA 925210001

Sub Contractor Numbers (c):

Patent Clause Number (d-1):

Patent Date (d-2):

Work Description (e):

Sub Contract Award Date (f-1):

Sub Contract Est Completion Date(f-2):

1 a. University of California - Riverside

1 b. 200 University Office Building

Riverside CA 925210001

Sub Contractor Numbers (c):

Patent Clause Number (d-1):

Patent Date (d-2):

Work Description (e):

Sub Contract Award Date (f-1):

Sub Contract Est Completion Date(f-2):

1 a. University of California - Irvine

1 b. 5171 California Avenue, Suite 150

Irvine CA 926977600

Sub Contractor Numbers (c):

Patent Clause Number (d-1):

Patent Date (d-2):

Work Description (e):

Sub Contract Award Date (f-1):

Sub Contract Est Completion Date(f-2):

1 a. University of California - Irvine

1 b. 300 University Tower

Irvine CA 926972725

Sub Contractor Numbers (c):

Patent Clause Number (d-1):

Patent Date (d-2):

Work Description (e):

Sub Contract Award Date (f-1):

Sub Contract Est Completion Date(f-2):

1 a. Pennsylvania State University

1 b. Office of Sponsored Programs
110 Technology Center Building
University Park PA 168027000

Sub Contractor Numbers (c):

Patent Clause Number (d-1):

Patent Date (d-2):

Work Description (e):

Sub Contract Award Date (f-1):

Sub Contract Est Completion Date(f-2):

1 a. Pennsylvania State University

1 b. 110 Technology Center
University Park PA 168027000

Sub Contractor Numbers (c):

Patent Clause Number (d-1):

Patent Date (d-2):

Work Description (e):

Sub Contract Award Date (f-1):

Sub Contract Est Completion Date(f-2):

1 a. Pennsylvania State University

1 b. Applied Research Laboratory
State College PA 168040030

Sub Contractor Numbers (c):

Patent Clause Number (d-1):

Patent Date (d-2):

Work Description (e):

Sub Contract Award Date (f-1):

Sub Contract Est Completion Date(f-2):

1 a. University of Utah

1 b. 75 South 2000 East
Salt Lake City UT 841128930

Sub Contractor Numbers (c):

Patent Clause Number (d-1):

Patent Date (d-2):

Work Description (e):

Sub Contract Award Date (f-1):

Sub Contract Est Completion Date(f-2):

1 a. University of Utah

1 b. 1471 East Federal Way
Salt Lake City UT 841021821

Sub Contractor Numbers (c):

Patent Clause Number (d-1):

Patent Date (d-2):

Work Description (e):

Sub Contract Award Date (f-1):

Sub Contract Est Completion Date(f-2):

1 a. University of Pittsburgh

1 b. 123 University Place
B21 UCLUB
Pittsburgh PA 152132303

Sub Contractor Numbers (c):

Patent Clause Number (d-1):

Patent Date (d-2):

Work Description (e):

Sub Contract Award Date (f-1):

Sub Contract Est Completion Date(f-2):

1 a. University of Pittsburgh

1 b. 350 Thackeray Hall
139 University Place
Pittsburgh PA 152602600

Sub Contractor Numbers (c):

Patent Clause Number (d-1):

Patent Date (d-2):

Work Description (e):

Sub Contract Award Date (f-1):

Sub Contract Est Completion Date(f-2):

Inventions (DD882)

Scientific Progress

Technology Transfer

Part of our work is aimed at designing antennas which are optimal in terms of allowing reliable communications in difficult wireless channels. This work represents a key enabler for the creation of reconfigurable antennas which can adapt to changing propagation environments. Because of our recent developments in this area, we are working with Rayspan Corporation, a start-up company with venture capital funding, to develop miniature reconfigurable antenna technologies for use in wireless networks. This collaboration has led to the creation of student projects (which will begin January 2009) as well as an upcoming summer visit by Prof. Jensen to Rayspan (summer 2009). The results of these projects will be the commercial deployment of the antennas for products in the consumer marketplace.

We have completed our flight tests with the US DoD at Cairns Field/Ft. Rucker, Patuxent River Naval Air Station, Edwards Air Force Base, and Pt. Mugu Naval Air Station. These tests have included channel sounding to test the wireless air-to-ground channel from multiple antennas on a helicopter and fixed-wing aircraft to multiple antennas on the ground. We have also implemented real-time space-time coding for this channel during some of these flight tests. This has demonstrated the use of multi-antenna signaling to overcome channel impairments observed in these air-to-ground communication channels.

We have completed measurements with Ericsson Research in Kista, Sweden with multiple coherent base stations communicating with mobile terminals. This has led to a detailed analysis of cooperative MIMO in urban environments.

Finally, we are working with a start-up company names Symmetry Wireless in Midway, UT. We are helping them develop liquid antenna technologies that can reconfigure themselves to adapt to different frequency bands or to different channel conditions. We have interest from several major handset manufacturers in this technology. The technology is also being used for ease of manufacturability by putting the liquid antennas in a case. This is being pursued by a variety of device manufacturers.

Scientific Progress and Accomplishments

In this section, we discuss the scientific progress and accomplishments made during the period of the proposed research project.

1. Physical Layer Techniques for Secure and Robust Communication: Key Establishment, Authentication, and Coding

Secret Key Establishment

Our initial research in this area focused on how to use the channel transfer coefficients in a MIMO link to generate secret keys for encryption. The basic motivation for this work is that communication over the MIMO radio channel requires estimation of the channel transfer functions between each pair of antennas. Alice and Bob, our two trusted nodes, can each estimate these transfer functions without revealing any secret information and then quantize these complex values appropriately to establish a secret key. The eavesdropper Eve can certainly estimate her channel to either of the two trusted nodes. However, these channels do not reveal information regarding the channel between Alice and Bob, and therefore Eve's knowledge of her own channel does not compromise the secrecy of the established key.

The thrust of the prior research was to demonstrate how to use the correlated random variables in a MIMO link to generate keys with independent bits. This work has been well received by the scientific community. However, one challenge with this approach for key establishment is that it requires the channel to change in time in order to generate keys of practical length. Therefore, generation of keys when the channel is essentially static remains an unsolved problem.

Our recent activities in this area have focused on using reconfigurable antennas to allow establishment of long keys in static or slowly-varying environments. Specifically, because the antenna radiation pattern becomes part of the radio channel, if this pattern can be reconfigured, each combination of transmit and receive patterns will excite/sample the channel in different ways, resulting in unique channel transfer functions for each pattern pair. But given a set of reconfigurable antenna modes coupled with a channel response (multipath propagation), the question becomes how to best use the reconfiguration to generate keys.

Our research has shown that given a power constraint used for the channel estimation, the optimization problem for determining the optimal allocation for each pair of modes is non-convex. However, we have developed a novel technique for determining this power allocation, and have been able to demonstrate the advantage of using optimal power allocation for channel estimation over traditional channel estimation where equal power is devoted to estimation of each channel coefficient. Figure 1 shows the number of bits achievable using this optimal power allocation compared to the number of bits achievable using equal power allocation as a function of the number of antennas in the arrays and the signal-to-noise ratio (SNR). As can be seen, for larger number of antennas, the optimal power allocation can have a significant impact on the performance. We are currently finalizing this research and working to extend it to practical reconfigurable antenna geometries.

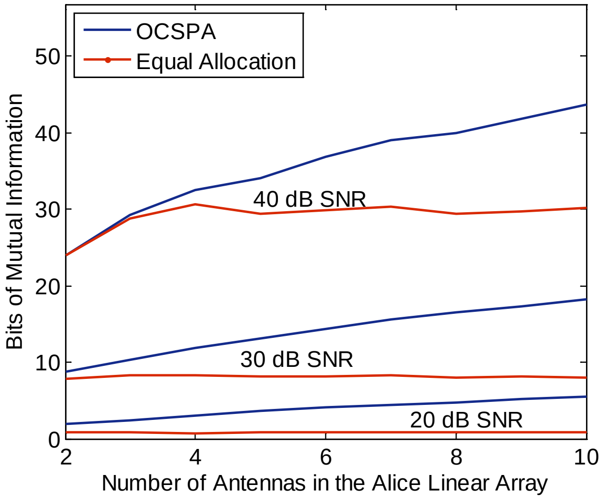


Figure 1: Number of bits in the secret key as a function of the number of antennas possessed by Alice and Bob for optimal power allocation (OCSPA) and equal power allocation in the channel estimation procedure.

Authentication

We have focused on the use of imperfections in MIMO radio transmissions to be able to uniquely identify different radios as part of an authentication procedure. Our work has emphasized imperfections in the modulated waveform. To conduct this research, we first used a vector signal analyzer to measure the features of the modulated waveform from each of the 3 antenna ports on 21 MIMO network interface cards (NICs). Features such as error vector magnitude, carrier frequency offset, and symbol clock error were recorded as a function of time.

Armed with this data, we then developed a minimal-redundancy maximal-relevance (mRMR) technique that orders the measured features in terms of their ability to uniquely identify the radios. This technique uses the average mutual information of different features as well as the mutual information between the features and the device identification. Portions of the data were then used to train a nonlinear classifier based on the bootstrap aggregating (bagging) algorithm with a decision tree kernel.

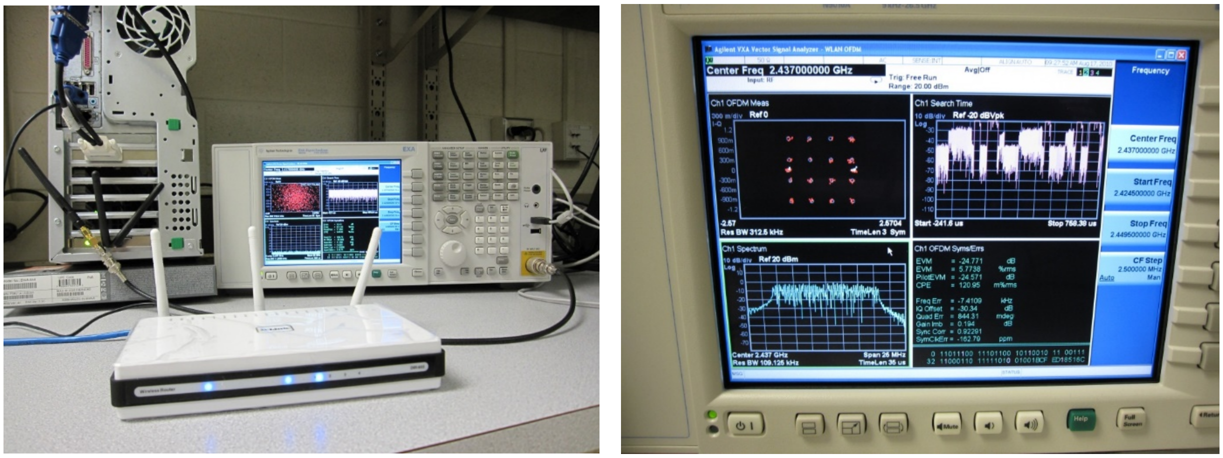


Figure 2: Measurement of the radiometric features of 21 MIMO NICs using a vector signal analyzer.

With the classifier trained, other portions of the data were used as inputs to the classifier to determine its ability to uniquely identify each radio. Figure 3 shows the precision of this classification, which represents the average ability to uniquely identify each radio, as a function of the number of features. As can be seen, for up to 3 features, the precision for MIMO and SISO (single antenna) is identical. However, as the number of features used in the classification increases, the enriched feature set provided by the MIMO radio allows it to be nearly perfectly accurate. This figure also shows the worst true-positive rate, which represents the identification accuracy for the NIC that is most-frequency incorrectly classified. Here again, classification based on MIMO radios significantly outperforms that based on SISO radios as the number of features becomes larger than 3.

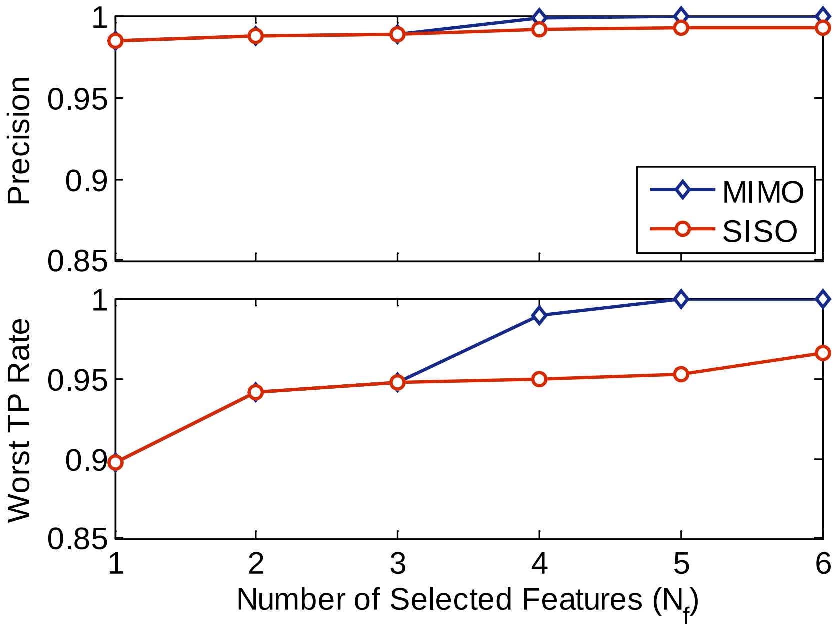


Figure 3: Classification precision and worst true-positive rate as a function of the number of features used to perform the classification for both MIMO and SISO radios.

This work has also explored the impact of feature drift as a function of time and temperature. Preliminary results show that classification using MIMO radios shows reduced sensitivity to such drift. Ongoing work is aimed at better understanding the impact of this drift and identifying methods for improved classification in light of the uncertainty generated by the drift.

Space-Time Coding

Finally, we have worked with Ericsson Research in Kista, Sweden to perform measurements where the channels from three base-stations separated by 0.5 to 1 km can be coherently measured to a single mobile subscriber using LTE signaling. These are the first measurements of their kind, and are designed to demonstrate how coherent cooperation between base stations can improve the communication reliability and throughput in urban macrocellular environments.

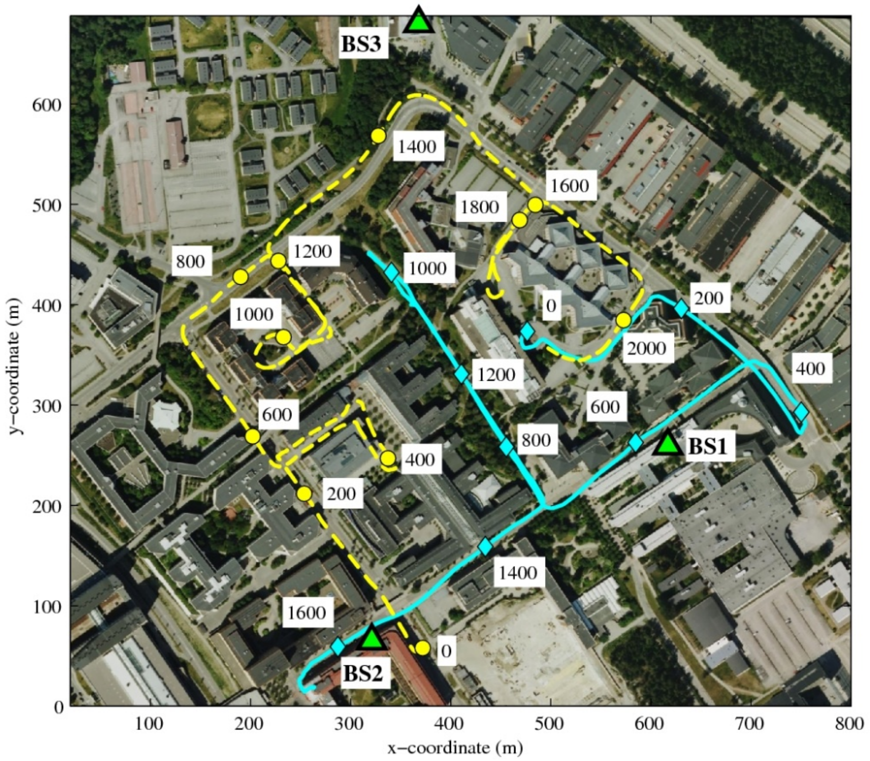


Figure 4: Measurement routes followed by the mobile subscriber for the cooperative MIMO communications channel sounding as well as the three base station (BS) locations.

Based on this measured data, we have explored in detail the impact of using cooperative MIMO communication for both single user (one mobile) and multiuser (two or three mobiles) scenarios. The results show that for point-to-point communication, cooperative signaling increases the communication capacity by 53% over that achieved using a single base station to communicate with the mobile. For downlink and uplink multiuser signaling, cooperative signaling provides a relative increase in performance of 91% and 63%, respectively. We have explored in detail channel eigenvalues, channel gains, and other relevant metrics to describe the channel. We have also demonstrated simple models that allow description of this type of channel for simulation and analysis of different coding schemes.

As part of this work, we have also developed a simple space-time coding algorithm that exploits the full covariance of the observed channel. This is in contrast to existing algorithms that make assumptions regarding a separable structure of the covariance. The advantage of this technique is that is allows determination of the optimal transmit strategy based upon the capabilities of the receiver, whereas past algorithms require an optimal receiver to achieve performance (minimum mean-squared error (MMSE) beamformer with nonlinear successive interference cancellation). Our approach is able to achieve near optimal performance with a simple MMSE receiver.

In another parallel effort, we investigated location distinction, the ability of a receiver to determine when a transmitter has changed location, which has application for energy conservation in wireless sensor networks, for physical security of radio-tagged objects, and for wireless network security in detection of replication attacks. Specifically, we investigate the use of a measured temporal link signature to uniquely identify the link between a transmitter (TX) and a receiver (RX). When the TX changed location, or if an attacker at a different location assumed the identity of the TX, the proposed location distinction algorithm reliably detected the change in the physical channel. This detection could be performed at a single RX or collaboratively at multiple receivers. We used 9,000 link signatures recorded at different locations and over time to demonstrate that our method significantly increased the detection rate and reduces the false alarm rate, in comparison to existing methods. We presented a procedure to estimate the mutual information in link and link signature using the Edgeworth approximation. For the measured data set, we showed that approximately 66 bits of link information is contained in each measured link signature.

Perimeter distinction in a wireless network is the ability to distinguish locations belonging to different perimeters. It is complementary to existing localization techniques. A drawback of the localization method is that when a transmitter is at the edge of an area, an algorithm with isotropic error will estimate its location in the wrong area at least half of the time. In contrast, perimeter distinction classifies the location as being in one area or the adjacent regardless of the transmitter position within the area. We used the naturally different wireless fading conditions to accurately distinguish locations across perimeters. We examined the use of two types of wireless measurements: received signal strength (RSS) and wireless link signature (WLS), and proposed multiple methods to retain good distinction rates even when the receiver faces power manipulation by malicious transmitters. Using extensive measurements of indoor and outdoor perimeters, we found that WLS outperforms RSS in various fading conditions. Even without using signal power WLS could achieve accurate perimeter distinction up to 80%. When we trained our perimeter distinction method with multiple measurements within the same perimeter, we were able to improve the accuracy of perimeter distinction, up to 98%.

We proposed and evaluated a new approach for secret key extraction where multiple sensors collaborate in exchanging probe packets and collecting channel measurements. Essentially, measurements from multiple channels have a substantially higher differential entropy compared to the measurements from a single channel, thereby resulting in more randomness in the information source for key extraction, and this in turn produces *stronger* secret keys. We also explored the fundamental trade-off between the quadratic increase in the number of measurements of the channels due to multiple nodes per group versus a linear reduction in the sampling rate and a linear increase in the time gap between bidirectional measurements. To experimentally evaluate collaborative secret key extraction in wireless sensor networks, we first built a simple, yet flexible testbed with multiple TelosB sensor nodes. Next, we performed large-scale experiments with different configurations of collaboration. Our experiments showed that in comparison to the 1X1 configuration, collaboration among sensor nodes significantly increased the secret bit extraction per second, per probe, as well as per mJ of transmission energy. In addition, we showed that the collaborating nodes could improve the performance further when they exploited both space and frequency diversities.

Measurements of received signal strength (RSS) on wireless links provide position information in various localization systems, including multilateration-based and fingerprint-based positioning systems, and device-free localization systems. Existing localization schemes assume a fixed or known transmit power. Therefore, any variation in transmit power can result in error in location estimation. We developed a generic framework for detecting power attacks and identifying the source of such transmit power variation. Our results showed that we could achieve close to zero missed detections and false alarms with RSS measurements of 50 transmissions only. We also analyzed the trade-off between accuracy and latency of detection for our method.

Modeling the Time-Variant MIMO Channel

Our goal is to explore the extension of conventional MIMO channel modeling techniques to time-varying channels by extracting model parameters from measured data and using information theoretic metrics to determine if the models capture the correct channel behavior. In the past, we have focused on (1) a random matrix model following the multivariate complex normal (MVCN) distribution and (2) a physical time-variant clustering (TVC) model [1]. However, in our prior implementation of the TVC model, we did not identify a stochastic description of the cluster behaviors. In this work, we have extended the TVC model to include an auto-regressive (AR) model for the multipath cluster parameters.

The basic model development is based on extracting the angle of departure, angle of arrival, and power gain of the dominant multipath clusters from measured data. The time evolution of these parameters are then used to create a stochastic description involving a probability density function (pdf) and power spectral density (PSD), which is a representation of the temporal correlation function. An auto-regressive model for the cluster time variation is created based on the stochastic description. Finally, the time-varying cluster model is used with antenna configuration information to create MIMO channel matrices whose time-variation matches that of the measured data.

The multivariate nature of the channel matrix complicates efforts of validating the model against the measured data. In this work, we adopt the approach from our prior work of comparing the values of established measures for quantifying the level of MIMO channel time variation generated from the model to those obtained directly from the measured channel matrices. The transmit capacity delay (TCD) approximates the capacity loss that occurs at time sample *k* when the transmitter forms its signaling strategy using the CSI at time sample 0. Similarly, the receive capacity delay (RCD) approximates the capacity loss that occurs when both the transmitter and receiver use outdated CSI in their signaling strategy.

Figure 5 plots the TCD and RCD normalized to a peak value of unity as a function of receiver node displacement computed from both the measured (averaged over all measurements) and modeled (averaged over 3000 channel realizations) data. As can be seen, if multipath clusters are allowed to appear and disappear (birth/death), the model is highly accurate in matching the measurements.

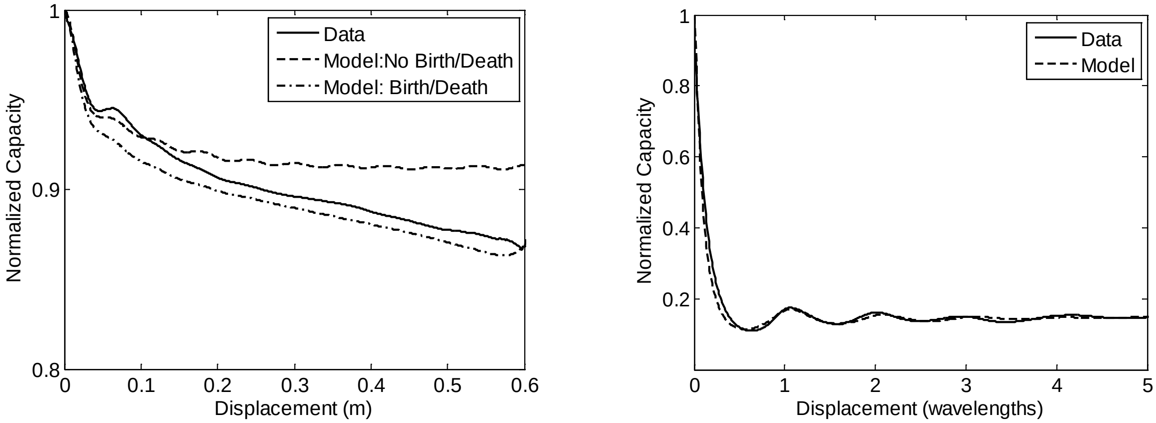


Figure 5: Normalized average (a) TCD metric and (b) RCD metric as a function of receiver displacement computed from the original measured data and the time-variant model.

The multi-user, multiple-input multiple-output (MIMO) broadcast channel has recently been the subject of tremendous interest, resulting in the development of the sum-capacity achieving non-linear dirty paper coding (DPC) as well as reduced-complexity and sub-optimal linear precoding (beamforming or BF) methods. However, these methods show sensitivity to inaccurate or outdated channel state information at the transmitter, and therefore their performance can degrade significantly in realistic operational environments.

Motivated by the performance loss suffered by outdated CSI in time-varying environments, we have recently developed a linear precoding strategy based on channel distribution information (CDI) at the transmitter, in the form of spatial correlation matrices that offers stable performance in the time-varying MIMO broadcast channel. We have extended this technique and analysis to the frequency-selective channel.

In this analysis, each receiver is assumed to possess perfect CSI at all frequencies. In contrast, however, the transmitter in the case of DPC or CSI-based beamforming chooses its precoding vectors for all frequency bins based on the CSI at the lowest frequency. In the case of CDI-based beamforming, the correlation matrix is similarly computed based on the data at the lowest frequency bin. In all cases, the sample expected throughput (SET) for the network as a function of frequency offset is averaged over the time series and all starting frequencies in the measurement for fixed network parameters and total transmit power level P.

Figure 6 plots the SET versus frequency offset using two different datasets from the indoor environment for $N_t = 5$ transmit antennas and $N_u = 5$ users. The total allocated power is fixed at $P = 10$. In both cases, the results reveal that DPC has the highest throughput under perfect CSI but is also highly sensitive to changes in CSI as a function of frequency. CSI-based beamforming similarly achieves high performance with perfect CSI, but this performance also falls dramatically with frequency displacement. However, when CDI-based beamforming weights are used, the throughput remains quite stable with frequency variations. As a result, its performance is superior to that offered by either DPC or CSI-based beamforming for frequency offsets beyond 10 MHz.

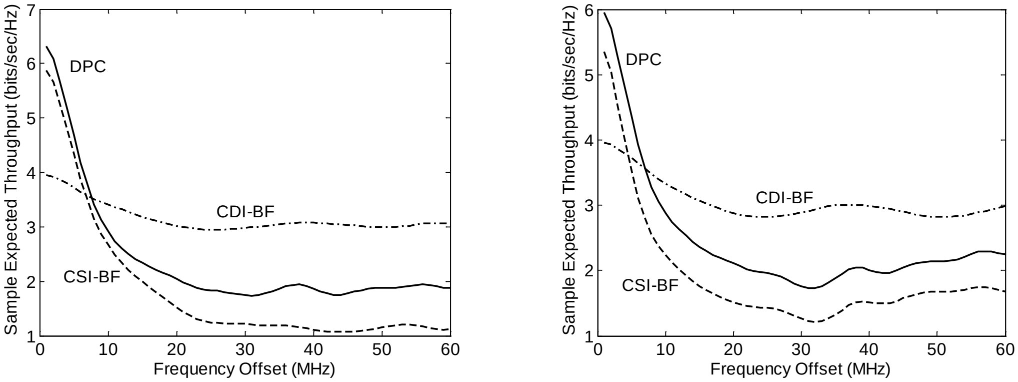


Figure 6: SET as a function of frequency offset for DPC, CSI-based beamforming (CSI-BF), and CDI-based beamforming (CDI-BF) for $N_t = N_u = 5$, $N_r = 1$, and $P = 10$ for two different channel measurements in an indoor environment.

Key Establishment using MIMO Channel Coefficients

One challenge in establishing a secure wireless link between network nodes is the establishment of encryption keys without allowing an eavesdropper the opportunity to obtain information that will help in determining the key. One idea that has been used recently in the literature is the establishment of keys based on the channel state information (CSI) between the transmitter (Alice) and intended receiver (Bob) since this CSI is not known to the eavesdropper (Eve). However, when evaluating the previous work on this topic, we find that each technique suffers from significant weaknesses.

This work presents practical methods for key generation using MIMO channels and analyzes their performance. First, assuming the target and eavesdropper channels to be correlated multivariate Gaussian, the theoretical limit on the number of key bits per random channel realization is derived along with the number of these bits that are “safe” from an eavesdropper. Second, two practical algorithms for key generation are considered and compared in terms of their complexity, efficiency in generating key bits, and security. In future work, we will use three node (transmitter, receiver, eavesdropper) measurements to evaluate the performance of the methods and the theoretical limits for real-world channels. For the sake of brevity, we will simply summarize the two practical algorithms in this report.

Channel Quantization Methods: A simple method for generating a random key at nodes 1 and 2 is for the two nodes to perform channel quantization (CQ) simultaneously on the channel between Alice and Bob. The total space of observable channels is divided into regions of equal probability, each with a unique assigned bit pattern. Due to estimation error at the two nodes, sometimes the key bits will not match, necessitating some kind of error correction over a public channel. This idea is extended to MIMO channels by performing CQ on each of the elements of spatially whitened stacked channel matrices. The main drawback of simple CQ is that channels on the region boundaries cause frequent key mismatch, perhaps too frequent for standard error control techniques. As a result, several variants of the technique which are less prone to error are included in the development.

Random Pre-Equalization: Although the channel-quantization methods are simple to implement and secure for independent channels, they suffer from fairly low efficiency relative to theoretical limits. Another possibility for generating random key bits is for Alice to generate vectors of random key symbols **E** according to some constellation and precode this using **U** = **HE**. The matrix **U** is sent to the Bob who can decode it using his knowledge of the channel matrix. Although the method has potentially higher efficiency than CQ methods, the main drawback is the higher complexity required to estimate and precode before the channel changes. Furthermore, this technique requires (1) careful selection of the key matrix **E** to achieve desired information theoretic characteristics and (2) hashing of bits based on what the eavesdropper can potentially learn from the transmission (based on a mutual information theoretic analysis that involves the eavesdropper's channel from the transmitter).

2. Security Techniques for Cryptographic Resistant Attacks

Cryptographic resistant attacks in mobile ad hoc networks (MANETs) such as jamming, physical layer wormholes, and malicious packet dropping are a growing concern and difficult to overcome. Here we briefly describe progress on developing security techniques to mitigate wormholes and malicious packet dropping. Physical layer wormhole attacks in ad hoc and sensor networks, can be launched regardless of the MAC, routing, or security protocol used in the network. Here, an attacker will place two transceivers M1 and M2 at two different locations in the network as shown in Fig.7. The transceivers M1 and M2 are connected through a link (wired or long range wireless link) referred to as the wormhole link. The transceivers capture packets or signals from one location and replay them at the other location. The wormhole link will be considered by legitimate nodes in the network as a short path from one side of the network to the other side (e.g., nodes B, 6, 7, and 14 in Fig. 7 will assume that nodes C, 8, 9, and 10 are one-hop neighbors). Consequently, the wormhole will attract a large amount of traffic between various source and destination nodes in the network.

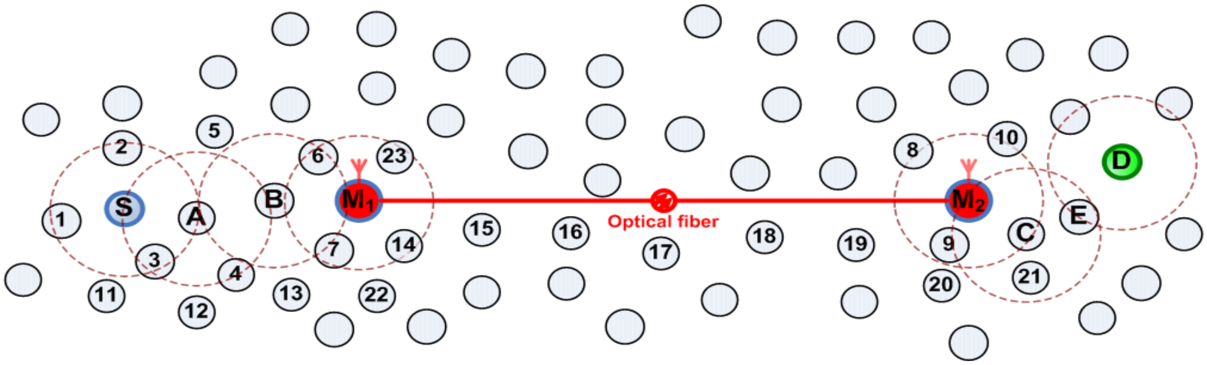


Fig. 7. Wormhole detection example

Most techniques proposed to detect this attack require precise and accurate information about the location of nodes, the time of packet transmission, or the use of special hardware. These requirements make such defense mechanisms expensive or complex. Other solutions that eschew such complexities cannot detect specific types of wormholes, especially physical layer wormholes. We developed "DeWorm", a novel, yet simple protocol to effectively detect wormhole attacks. DeWorm employs routing discrepancies between neighbor nodes to detect wormhole attacks. Specifically, for each node pair one hop apart along the current source/destination working route DeWorm finds an alternate route avoiding nodes in working route and neighbors of source. It then compares the length of alternate routes to the current working route, if the length of the alternate route is above a sensitivity parameter threshold, then a wormhole is detected. Our analysis and simulations show that the proposed protocol can detect wormhole attacks with nearly 99% detection rates and very few false positives. Furthermore, in comparison to other wormhole detection protocols, the proposed protocol is simple, applied on demand when it is suspected that a wormhole may exist, localized, needs no special hardware, or synchronization, and is capable of detecting different types of wormhole attacks including physical layer wormholes.

Detecting malicious packet dropping is important in ad hoc networks to combat a variety of security attacks, such as, blackhole, greyhole, and wormhole attacks. We considered the detection of malicious packet drops in the presence of collisions and channel errors and describe a method to distinguish between these types. We present a simple analytical model for packet loss that helps a monitoring node to detect malicious packet dropping attacks. The model is analyzed and evaluated using simulations. The results show that it is possible to detect malicious packet drops in the presence of collisions and channel errors.

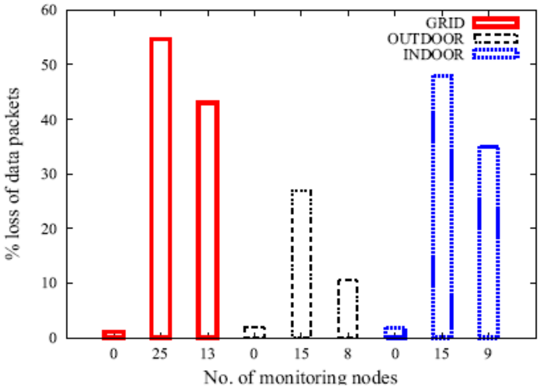
3. Topological Robustness and Monitoring

One approach to increase the resilience of mobile ad hoc networks (MANETs) and unstructured sensor networks is to deploy the network such that there are k-disjoint routes in the network between each pair of network nodes (i.e., k-connectivity). We have presented the results of a simulation study investigating the relationship between asymptotic results in the literature and k-connectivity under varying nodal density and nodal degree. The numerical results illustrate where the asymptotic approximations breakdown and we show that this largely due to the existence of critical connectivity points in the topology. Using a critical point identification algorithm we examine how the number of critical points varies with nodal degree, nodal density and node mobility.

We note that in order to effectively deploy techniques to improve the resilience of sensor networks and MANETs one must be able to identify all the weak points of a network topology. Here we define the weak or critical points of the topology as those links and nodes whose failure results in partitioning of the network. We have developed a novel algorithm to identify the critical points of a sensor and MANET topology based on results from algebraic graph theory. Unlike exiting algorithms in the literature, the technique has the advantage of being able to study the effects of any combination of failures (links, or nodes, multiple failures) and scales with the network information available. Using this algorithm, we have studied the effects of network density, node mobility and limited topology information on the existence and identification of critical connectivity points.

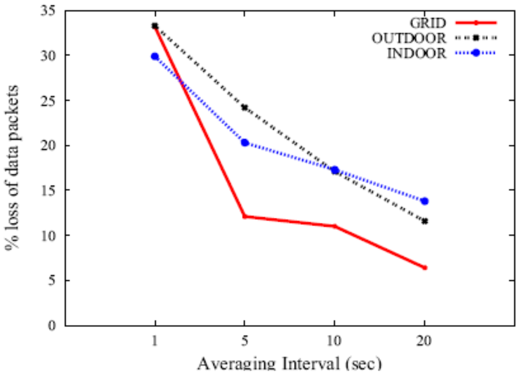
In another work, we have looked at the issue of efficient monitoring in WMNs. Effective management of WMNs requires an underlying monitoring framework, which collects the necessary statistics from the wireless network. However, the impact of monitoring overheads on the transmission of data traffic in wireless networks has not been studied so far. Thus, we study the impact of monitoring traffic on the forwarding of user data traffic, for different applications. We then evaluate the performance of several schemes for reducing the monitoring overheads in WMNs. We also investigate whether these techniques impact the desired functionality for which the network is being monitored.

We propose three different approaches for efficient monitoring in WMNs: i) Monitor Selection approach, ii) Reporting Interval approach, and iii) Threshold-based monitoring. We evaluate our proposed schemes using the QualNet simulator, for three different topologies, two of which are adapted from real-world testbeds. We evaluate as to how these schemes help us in reducing overheads (thereby improving the end users' performance), and their impact on the desired functionality



Topology	No. of monitoring nodes	Avg. Throughput (Mbps)	Avg. Delay (sec)
GRID	25	1.16	0.72
	13	1.25	0.68
OUTDOOR	15	1.27	0.70
	8	1.42	0.62
INDOOR	15	1.03	1.17
	9	1.15	0.94

Fig.8. Pkt. loss for monitor selection approach   Table 1 Perf. of AODV for monitor selection approach



Topology	Reporting Interval (sec)	Avg. Throughput (Mbps)	Avg. Delay (sec)
GRID	1	0.86	0.82
	10	1.09	0.64
OUTDOOR	1	0.97	0.48
	10	1.25	0.34
INDOOR	1	1.03	1.17
	10	1.24	0.95

Fig.9 Pkt. loss for reporting interval approach Table 2 Perf. of AODV for reporting interval approach.

Security through Clock Skew Measurements and Other PHY layer Characteristics

- We explored the use of clock skews to detect unauthorized access points in wireless local area networks. We developed a methodology that benefits from higher precision timestamps and higher predictability in a local area setting. We evaluated this methodology using traces from the ACM Sigcomm 2004 conference, and two, different residence areas. We showed that our high precision skew estimation is an order of magnitude faster and uses an order of magnitude less packets compared to the existing

TCP/ICMP based techniques. We also discussed and quantified the impact of various external factors including temperature variation, virtualization, and NTP synchronization, on clock skew. We also explored the possibility of engineering clock skews to allow a fake AP to generate the clock skew of the original one. Our exploration results indicate that the use of clock skews appears to be an efficient and robust method for detecting fake APs in WLANs.

- We explored the opportunity to use sophisticated PHY-layer measurements in wireless networking systems for location distinction. We first compared two existing location distinction methods - one based on channel gains of multi-tonal probes, and another on channel impulse response. Next, we combined the benefits of these two methods to develop a new link measurement that we call the complex temporal signature. We used a 2.4 GHz link measurement data set, to evaluate the three location distinction methods. We found that the complex temporal signature method performs significantly better compared to the existing methods. We also performed new measurements to understand and model the temporal behavior of link signatures over time. We integrated our model in our location distinction mechanism and significantly reduced the probability of false alarms due to temporal variations of link signatures.

- We have built a new methodology to exchange a nearly perfect random secret key between two parties exploiting the inherent randomness and the reciprocity of the wireless channel between them. Specifically, we measured and used the time-variation of the received signal strength (RSS) as the statistic of the radio channel and the source of secret information shared between a transmitter and receiver. We used two novel techniques from quantum cryptography, information reconciliation and privacy amplification, for improving the performance and security of our scheme. We also proposed and evaluated different methods for information reconciliation to achieve a faster key generation rate. We implemented our scheme on three laptops with wireless sensors that we used to measure the RSS over time. Our implementation showed that our methodology allows two nodes to quickly and securely extract a secret from the channel measurements with minimal overhead.

4. Coping with Jamming Attacks

One of our tasks was focused on understanding the effects of and coping with jamming attacks. Towards this we first quantify the effectiveness of previously proposed methods for mitigating the jamming effects. In particular, we focus on frequency hopping which is the most popularly considered anti-jamming method and the only one implemented in real systems up to now. We design and implement a measurement driven anti-jamming system, which effectively alleviates the impact of a jammer and overcomes the deficiencies of frequency hopping. We summarize our achievements below.

1. **Quantifying the efficacy of frequency hopping in coping with jamming attacks.** By employing frequency hopping the communication link tries to avoid the presence of a jammer by changing its band of operation. However there are two factors that impact the effectiveness of this strategy. These are: (a) the number of orthogonal channels available for use and (b) the frequency separation between these orthogonal bands. If the latter is small, then the energy spill over between two adjacent orthogonal bands can be large to cause failures of packet receptions at the receiver, as well as to trigger the CSMA/CA back-off mechanism at the transmitter. Towards quantifying the efficacy of this scheme in a wireless network we construct a measurement driven, game theoretic framework that accounts for both the above limiting factors. We perform an extensive set of experiments on our indoor 802.11 testbed in order to obtain the measurements required to drive our framework for the case of 802.11 systems. In particular, these measurements quantify the impact of a jammer on an 802.11a/g communication link. Based on these measurements we apply our framework and our results (both analytical and experimental) indicate that frequency hopping is

inadequate in coping with jamming attacks in current 802.11 systems. We also evaluate the efficacy of frequency hopping if the systems were to have a larger number of frequency bands. We find that the system has to have about 100 bands in order for it to be effective against a single jammer.

2. **ARES: an Anti-jamming REinforcement System for 802.11.** We first conduct an extensive set of experiments on our indoor wireless testbed in order to assess the ability of two physical layer functionalities – rate and power control - in mitigating jamming. We find that in the presence of a jammer: (a) the use of popular rate adaptation algorithms can significantly degrade network performance and (b) appropriate tuning of the Clear Channel Assessment (CCA) threshold allows a transmitter to send packets even when being jammed and enables a receiver to *capture* the desired signal. Based on these findings we build our anti-jamming system, ARES. ARES tunes the parameters of rate adaptation and power control to improve the performance in the presence of jammers. We implement and evaluate our system in three wireless testbeds: (a) an 802.11n WLAN with MIMO nodes, (b) an 802.11a/g mesh network with mobile jammers and (c) an 802.11a WLAN. We observe that ARES improves the network throughput across all testbeds by up to 150%. Furthermore, ARES ensures (i) that operations are unaffected under benign conditions and (ii) that is effective in cases where frequency hopping is unable to mitigate jamming (e.g. under the presence of a wideband jammer).

Evaluating Frequency hopping as a Jamming mitigation technique:

A jammer is a malicious entity, which purposefully emits electromagnetic energy on the medium in order to disrupt ongoing communications. The most popularly considered approach for alleviating the jamming effects is frequency hopping. In this work we develop a framework to quantify the effectiveness of this strategy in any given wireless technology. In a nutshell our contributions are:

a) Construction of a measurement-based game theoretic framework to bound the performance of proactive frequency hopping in the presence of a jammer. We model the interactions between the link and the jammer as a two player, zero sum game.

b) Quantifying the impact of a jammer via experiments on an indoor wireless testbed with both 802.11a and 802.11g. The results of our experiments show that the presence of a jammer on an adjacent, albeit orthogonal channel to that of the legitimate pair can still significantly degrade the performance.

c) Applying our framework to quantify the efficacy of proactive frequency hopping in 802.11 networks. Our results indicate that proactive frequency hopping provides very limited protection to an 802.11 network, from jamming attacks.

Frequency hopping tries to avoid the jammer by switching between multiple orthogonal narrow bands. The method can be effective in the presence of a narrow band jammer, but there are two factors that limit its performance: (a) the number of available orthogonal bands and (b) the frequency separation between these orthogonal bands. We provide a game theoretic framework, which accounts for both the aforementioned factors and gives performance bounds for a proactive frequency hopping scheme.

We model the interaction between the communication link and the jammer as a zero sum two person game. Both players employ frequency hopping in order to achieve their objectives. The game in normal form is represented by a triplet $< N, \Sigma_i, A >$; N is the set of players, Σ_i is the set of strategies for player i and A is the payoff matrix. In our case, N contains the link and the jammer. Σ_i is the same for both players and it is the number of available orthogonal bands. Finally the payoff matrix is defined as following: A_{ij} is the percentage of the jamming-free throughput that the legitimate link enjoys when it resides on channel i and the jammer resides on channel j. With this definition of the payoff matrix the value (or payoff) of the game u is defined to be the percentage of the jamming free throughput that it is achieved on the link. On the one hand the link tries to maximize this payoff while on the other hand the jammers tries to minimize it. As a zero sum two-person game, there **always exists an equilibrium**.

In order to compute the equilibrium strategies let us assume that the link chooses its channel randomly, using a probability distribution (mixed strategy) x, while the jammer picks its channel from the probability distribution y. The value of the game is then simply $u = x^T A y$. The equilibrium strategies can be found by solving the following primal-dual linear programs:

$$\begin{array}{llll} \max imize & u & \min imize & u \\ s.t & A^T x \geq u & s.t. & Ay \leq u \\ & |x| = 1 & & |y| = 1 \\ & x \geq 0 & & y \geq 0 \end{array}$$

From the above formulation we can see that our framework accounts for both (i) the number of available channels of the wireless technology under consideration and (ii) the effectiveness of a jammer which resides in a different orthogonal band.

Measuring the impact of a jammer in 802.11 networks

In order to quantify the effect of a jammer on a communication link we conduct an extensive set of experiments on our testbed. In particular, we want to examine the effect of a jammer who resides on an orthogonal band to that of the communication. In order to do this we first initiate the communication on one of the orthogonal bands available. Subsequently, the jammer is turned on. The jammer sweeps the available orthogonal bands, one channel at a time. We measure the throughput of our legitimate communication in any case. We consider a large variety of topologies.

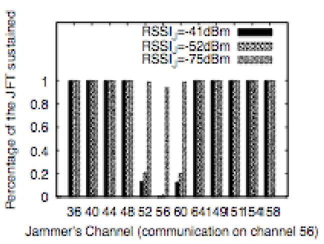
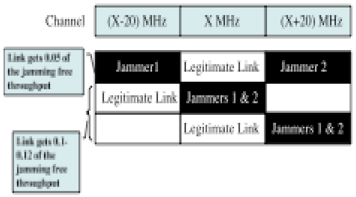
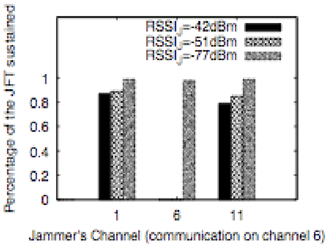
I. The case of 802.11a

In this case we have 12 orthogonal channels. In Figure 10 we present our results for one jammer and for the case that the legitimate link was using channel 56. In this case the RSSI on the link is -37dBm and we present the results for various RSSI values to the end points of the link from the jammer, in order to account for various topologies. Our main observation is that **a jammer, which transmits signals on an orthogonal band that is adjacent to that of the legitimate communication, can significantly degrade the throughput performance. Specifically, the throughput of the connection drops to approximately 10-15% of the jamming-free throughput** (the exact degradation depends on the distance between the jammer and the link and the characteristics of the channel). The reason for this may be attributed to the fact that RF filters do not provide sharp cut off at the specified boundaries of the channels.

Next we conducted experiments with two jammers. We considered all possible placements of the jammers on the 12 orthogonal that are supported from 802.11a. Our main observations are summarized in Figure 11. When the two jammers reside on the two orthogonal channels adjacent to that of the communication link, the degradation in the link throughput can be as high as 95%.

II. The case of 802.11g

In this case we have only 3 orthogonal channels. However, these channels have a spacing of 3MHz. Conducting the same set of experiments we can observe that, as with 802.11a, the presence of a jammer on an orthogonal, adjacent channel degrades the performance on the communication link. However as we note in Figure 12, where we depict some representative experimental results with 802.11g, the degradation is much lower than with 802.11a. This can be primarily attributed to the larger channel separation between the orthogonal bands; this results in a reduced seepage of the spectral power of the jammer into the adjacent channel being used by the legitimate communication. Note however, that since there are only 3 orthogonal channels in the 2.4GHz band, frequency hopping is not expected to provide significant benefits.

<table>
<tr>
<td>
</td>
<td>
</td>
<td>
</td>
</tr>
<tr>
<td>Fig 10. 802.11a (one jammer).</td>
<td>Fig 11. 802.11a (two jammers).</td>
<td>Fig 12. 802.11g (one jammer).</td>
</tr>
</table>

Applying our framework to 802.11 networks

Using the measurements we obtain from our testbed we formulate the corresponding payoff matrices as described earlier and we solve the corresponding linear programs. The results for 802.11a are presented in the following table.

# jammers	1	2	3	4
u	0.78	0.56	0.34	0.12

From this table we see that frequency hopping can restore 78% of the jamming free throughput when one jammer is present. However with 4 jamming devices appropriately placed on the frequency spectrum, one can basically block the whole 802.11a band. In particular, these jamming devices should be placed on channels 2, 5, 8, and 11 (we enumerate the channels from 1 to 12). Moreover, every equilibrium strategy for the link should avoid these 4 channels (given that the jammer is using the above strategy).

For the case of 802.11g we get the following table after solving the corresponding linear programs:

# jammers	1	2	3
u	0.61	0.29	0

We can observe that even if the impact of a jammer on an adjacent orthogonal channel is smaller with 802.11g, the small number of orthogonal bands is an extremely limiting factor. In order to see this more clearly we solve our game by calibrating the payoff matrix from our measurements. In particular, the effect of the jammer is kept the same but we expand the payoff matrices in order to account for more channels. Figures 13-15 present some characteristic results. In Figure 13 we can see that if current systems were to support a large number of orthogonal bands frequency hopping would be able to restore almost all of the jamming free throughput (one jammer present). Moreover the number of jamming devices needed in order to degrade the throughput further would be increased as we can see from Figures 14 and 15.

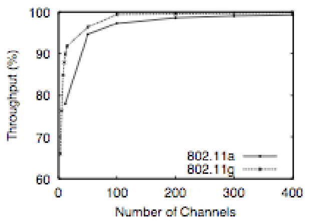
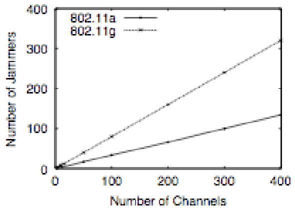
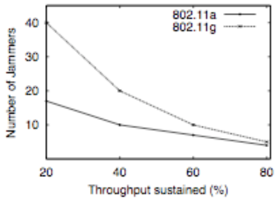
		

Fig 13. Throughput sustained with more channels.	Fig 14. Number of jammers needed to drop throughput below 20% of the jamming free.	Fig 15. Number of jammers needed to drop the throughput at a specific percentage (50 channels).

Finally, we implemented on our testbed a prototype proactive frequency-hopping scheme. We input hopping sequences obtained from the equilibrium strategies and we experiment with different *resident times* for the jammer and the link (RT_J and RT_L respectively). Our results, presented in figures 7 and 8, indicate that indeed, our framework provides bound on the performance of a proactive frequency-hopping scheme.

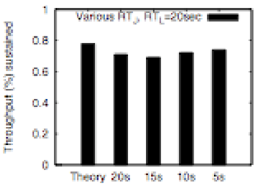
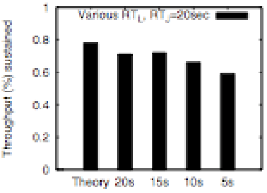
	

Fig 16. Varying RT_J	Fig 17. Varying RT_L

ARES: an Anti-jamming REinforcement System for 802.11

As discussed earlier, frequency hopping tries to avoid the jammer by changing band of operation and as a result it cannot be effective in scenarios that involve wide-band jammers and/or multiple jamming devices in the different orthogonal channels. In this part of the project, we first conduct experiments on our 802.11 indoor to assess the ability of two physical layer functions – rate and power control – in mitigating jamming effects. Based on our findings we design, implement and evaluate on our testbed a measurement driven anti-jamming system. In a nutshell, our main contributions are:

a) Understanding the impact of jammers in an 802.11 network with rate/power control. In particular we find that (i) rate control is not always beneficial under the presence of a jammer and (ii) tuning the CCA threshold can allow a transmitter to send packets even when being jammed and enables a receiver to capture the desired signal.
b) Design of a novel anti-jamming system, which we call ARES. The above observations drive the design of ARES. ARES consists of two modules, a **rate control** module which decides between fixed rate transmissions and rate control, and a **power control** module, which tries to tune the CCA threshold to facilitate the transmission and reception of legitimate packets during jamming.
c) Implementation and experimental validation of ARES. We implement and evaluate ARES on our testbed under various 802.11 configurations. Our measurements indicate that ARES provides throughput improvements in all cases considered; throughput improvements of up to 150% are observed.

Interaction between rate/power control and random jamming

In this work we mainly consider the *random jamming* model. A random jammer oscillates between active and idle period chosen from two (different) distributions. It is the most realistic jamming model since it enables the jammer conserve battery life and also makes its detection harder. Moreover, by appropriately tuning the jamming distributions we can get characterize all the jamming models possible (e.g. constant, deceptive, and reactive jammers).

We first want to study the interactions between the rate control employed on a communication link and the jammer. Our main observation is that **rate adaptation consumes a significant part of the jammer's sleep time, to converge to the appropriate rate.** As a result, **fixed rate assignment outperforms rate adaptation on links that can sustain high transmission rates under benign conditions.**

Figure 18 presents a time trace for a communication link when fixed rate transmissions at 54Mbps is used and when sample rate algorithm is used. We observe that sample rate consumes a very large amount of the jammer's sleeping time in order to converge to the best rate (if at all). At Figure 19 we present our average results for various fixed transmission rates and for various rate control algorithms implemented on the driver of our wireless cards.

Based on these observations we construct an analytical tool, which determines whether it is better to use a fixed, or an adaptive rate approach for a given link, based on the long-term throughput achieved with each strategy. In order to decide on this we need to know (a) the distribution of the jammer's sleeping and active period, (b) the application data rate, (c) the performance metric on the considered link (e.g. PDR), (d) the rate adaptation used, and in particular the time needed for the rate control algorithm to converge after a sudden decrease of the throughput and (e) the *effectiveness* of a jammer (measured in terms of throughput achieved on the link under the presence of the jammer). Note that one or more of these parameters might not be available. This can make our analytical tool (called ARC for Analytical Rate Control) difficult to be employed, however it gives us insights on the way that rate control is affected from a jammer. The insights obtained form the basis of a simpler and more practical (but less accurate) module described later. ARES invokes this module when we are unable to employ our analysis.

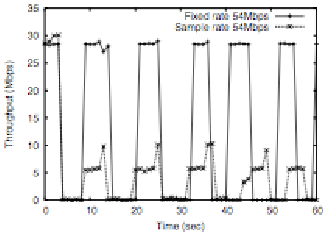
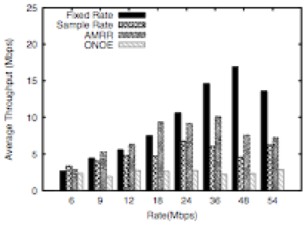
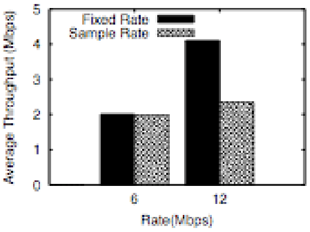
		

Fig 18. Rate adaptation may under-perform as compared to fixed rate transmissions.	Fig.19 High rate links perform better with fixed rate under jamming attacks.	Fig 20. Rate adaptation presents the same behavior in multi-hop settings too.

Next, we examine the impact of a random jammer on the end-to-end throughput of a multi-hop path. We place the jammer such that it affects one or more links. Along each route, links that are not affected by the jammer consistently use the rate adaptation algorithm. *On the links that are subject to jamming, our analysis dictates the decision on whether to use fixed or adaptive rate assignments.* In Figure 20, we show the throughput for routes on which, in the absence of jammer, end-to-end throughputs of 6 and 12 Mbps are achieved. From this figure we can see that **the behavior with rate adaptation in multi-hop routes, in the presence of a jammer, is the same as that on a single-hop link.**

Next we examine interactions between power control techniques and the presence of a jammer. In particular we want to study the impact of increasing the transmission power on the link (we denote this power with P_L and the corresponding transmission power of the jammer with P_J) as well as increasing the CCA threshold on the communication link (denoted with CCA_L). Our results indicate that **mitigating jamming effects by incrementing P_L is viable at low data rates. It is extremely difficult to overcome the jamming interference at high rates, *simply with power adaptation.*** Moreover, **increasing the CCA_L restores (in most cases) the isolated throughput (the throughput achieved in the absence of the jammer).**

Figure 21 depicts a subset of our experiments with power adaptation. Our measurements indicate that when high transmission rates are used, increasing P_L does not help alleviate the impact of jammers. In contrast, we observe that with low data rates and when P_J is low, data links can overcome jamming to a large extent by increasing P_L. Note also that when P_J is high, it is extremely difficult to achieve high average throughput.

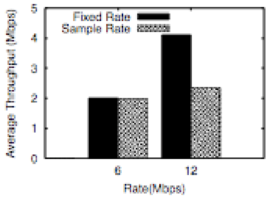
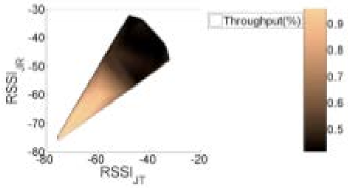
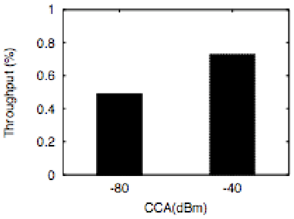
		

Fig 21. Increasing the power can only help in low	Fig 22. Increasing the CCA can help alleviate the jamming effects.	Fig 23. Increasing the CCA can help also in multi-hop settings.

transmission rates and low power jammers.		

In order to overcome the presence of a high power jammer (which is of more interest) we examine possible manipulations of the CCA. Our experiments indicate that tuning the CCA threshold is a potential jamming mitigation technique. Increasing the CCA helps the transmitter ignore the jamming signals that arrive at its circuitry with RSSI lower than the CCA, and consequently it transmits its packets ignoring the presence of the jammer. In addition, the receiver tries to decode only the signals that arrive at its antenna with RSSI higher than CCA. In Figure 22 we present the average throughput when we increase the CCA on the two end points of the link at -50dBm, for various RSSI values from the jammer at the receiver and the transmitter ($RSSI_{JR}$ and $RSSI_{JT}$ respectively). We use the maximum power on the link. We notice that when the RSSI from the jammer is smaller than -50dBm we are able to ignore almost completely the presence of the jammer and restore up to 95% of the jamming-free throughput.

Finally, we perform experiments with various CCA thresholds along a route (all links use the same increased CCA). We experiment with the same multi-hop settings as the one for rate adaptation. Figure 23 presents the results observed on one of the routes. We observe that careful CCA tuning can provide significant end-to-end throughput gains.

ARES is comprised of two modules based on our previous measurements. In particular there is (i) a rate control module and (ii) a power control module. The rate control modules decides between fixed or adaptive rate, while the power control module tries to set the CCA threshold such that it ignores jamming signals to the extent possible.

Rate control: Ideally we would use our analytical model for deciding between fixed and adaptive rates. However, in a real system some of the parameters required might not be available. This is the reason we built another module (which we call Markovian Rate Control – MRC), based on insights gotten from our measurements, that does not require any inputs.

Our rate control module applies ARC if all inputs are available. In any other case it employs MRC. MRC keeps track of the last rate used under benign conditions (i.e. sleeping period of the jammer), and as soon as the jammer becomes inactive again it sets this fixed rate. However since the wireless environment is dynamic, MRC invokes rescanning every *k* jamming cycles (where k is an implementation parameter). When *k*=1we do not expect to have any benefits, since the rate control algorithm is invoked in each cycle. MRC is simpler to implement (since it does not need any inputs), however it is less accurate.

Power control: The power control module measures the RSSI on the link and the RSSI from the jammer at the two end points of the link in order to compute the CCA to be set on the communication link. Moreover we need to have an estimation of the *shadow fading variation* Δ of the environment we deploy our network. If the RSSI from the jammer on the link is smaller than the RSSI on the link by at least Δ dBm, then we set the CCA on the link equal to this quantity, i.e. $RSSI_{link}$-Δ. Figure 24 presents a flow chart for our system.

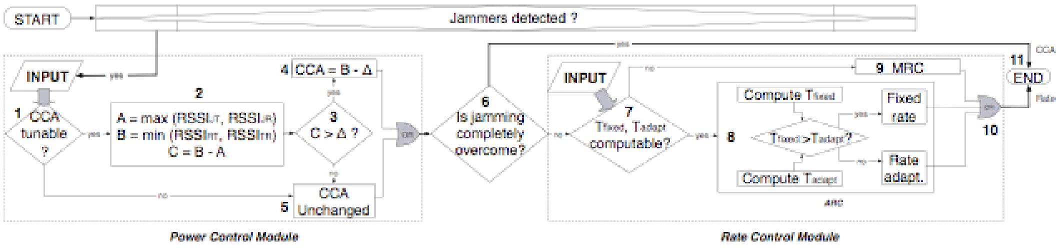


Fig 24. Flow chart of ARES

We evaluate ARES by examining its performance in three different networks: a WLAN comprised of MIMO-based links, a mesh network in the presence of mobile jammers and an 802.11a WLAN where uplink TCP traffic is considered.

Our results are presented in Figures 25-27. We notice that in all cases ARES can provide significant benefits. Note that in the case of 802.11n WLAN, our wireless cards do not allow us for tuning the CCA threshold. As a result ARES invokes only the rate control module.

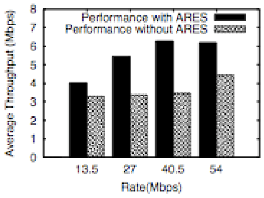


Fig 25. ARES provides benefits in an 802.11n WLAN.

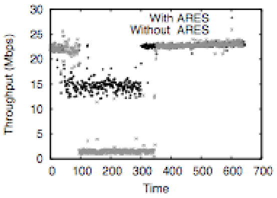


Fig 26. ARES mitigates the effects of a mobile constant jammer.

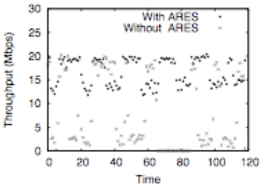


Fig 27. Performance of ARES in an 802.11a WLAN with TCP uplink traffic.

5. Secure Routing

Interest-Driven Approach to Secure, Integrated Unicast and Multicast Routing

There have been a large number of routing protocols proposed and implemented to date for secure routing in MANETs, and these prior approaches have focused on securing either paths or distances. Path-based approaches attempt to secure entire paths or have each node along the path attempt to secure the link it intends to use. This approach is not viable in large MANETs because it leads to unsustainable flooding of control packets, which can further degrade the performance of the network. In distance-oriented approaches, each node picks its next hop to a destination independently of other nodes, and this decision relies on some advertised metric and therein lies a fundamental security flaw. As long as this metric is something the node itself must advertise explicitly, adversaries can misrepresent their relative location and manipulate path discovery in their favor. Cryptography cannot be used to secure this information, given that the node itself is responsible for this metric, and its neighbors cannot determine the validity of the advertised information without complete path information. Our review of prior work on secure routing for MANETs indicates that, while the use of cryptography has been used to successfully counter some of these attacks, the solutions proposed to date do not guarantee that data packets are delivered, even if nodes comply with correct control signaling. Many attacks are aimed at forcing data to be routed through adversary nodes, and once this is done they can perform denial of service, or disclosure attacks.

Based on the above assessment of secure routing for MANETs, we are focusing on an approach built on three components: (a) algorithms for on-demand loop-free routing based on information that cannot be tampered on a hop-by-hop basis, (b) end-to-end feedback to source nodes that links the physical characteristics of paths used to deliver information to any advertised ordering based on such paths, and (c) use of path diversity to increase the probability that paths are found that have no adversaries. During this first year, we made substantial progress in Part (c) of our strategy, i.e., developing techniques to support path-diversity for secure routing by establishing multiple paths from sources to destinations very efficiently. The rest of this section summarizes the results we obtained in this area over the past year. We have also started to develop sufficient conditions for distributed loop-free routing that do not require verifiable explicit announcements of distance, path or link-state information by the neighbors of each node, and have started to analyze the role of end-to-end verification of routing information.

There have been many approaches to maintain efficient routing in MANETs. These approaches include organizing the network into clusters, reducing the rate at which signaling packets propagate away from the origin of an update, and using geo-location information to direct signaling packets to particular regions of the network. A careful review of the prior work reveals that (a) existing routing protocols for MANETs support either unicast routing or multicast routing, and (b) the dissemination of signaling traffic in MANETs is not closely linked to the interest that nodes have on destinations, and is structured as either strictly on-demand, strictly proactive, or the use of both types of signaling by dividing the network into zones. Over the past year, we have investigated the development of a unifying framework for all types of routing, and unicast and multicast routing in particular, and the use of interest in certain destinations (nodes, groups of nodes, roles, information objects, etc.) as the means to reduce signaling overhead. Our research has resulted in the design, verification and analysis of two new protocols, which we describe next.

Hydra: We first developed the Hydra multicast routing protocol, which was motivated by the desirability of providing the best features from the two alternatives in the existing design space for multicast routing in MANETs proposed to date.

Whether multicast routing protocols for MANETs build multicast trees or meshes, all of them are based on network-wide dissemination of control packets to inform the rest of the nodes about the existence of multicast groups. In receiver-initiated schemes, only one node, which in many schemes is called the core of the group, originates the dissemination of information about a multicast group reaching all other nodes, and receivers send explicit requests towards the core to join the group. This approach was originally introduced in the core-based tree (CBT) multicast routing protocol.

Hydra is the first sender-initiated multicast routing protocol that incurs the same order overhead as receiver-initiated approaches, and yet establishes multicast meshes that approximate routing structures containing the shortest paths from multicast sources to their destinations. Hydra creates a multicast mesh formed by a mixture of source-specific and shared sub-trees (or sub-meshes) using as few control packets as receiver-initiated schemes. The key ideas behind Hydra are: Restricting the dissemination of control packets to those regions of the network where other dynamically designated sender has previously discovered receivers, aggregating control messages from non-core senders, and electing a sender as the core in non-destructive manner. We have proven that the algorithm used in Hydra to perform multicast-state aggregation is correct (i.e., it establishes loop-free routes from sources to receivers). We used simulation experiments to compare Hydra's performance with that of ODMRP, which is the existing proposal for multicast routing in the IETF, by considering different numbers of sources, group sizes, node density and the use of 802.11 and TDMA as the underlying MAC protocol. The results demonstrate the performance benefits that should be expected from the approach implemented in Hydra, and that Hydra provides substantial performance improvements over ODMRP even in scenarios involving relatively small networks with few multicast sources. Hydra attains the same or better delivery ratios than ODMRP, and does so while transmitting from one third and one half the number of data packets sent in ODMRP and incurring end-to-end delays that are close to an order of magnitude smaller than in ODMRP.

PRIME: Based on our success with Hydra, we studied the integration of unicast and multicast routing a single protocol, and developed the Protocol for Routing in Interest-defined Mesh Enclaves (PRIME) . PRIME establishes and maintains a routing mesh for each active multicast group, i.e., for each group with active sources and receivers and for each unicast destination with at least one active source. The first source that becomes active for a given unicast or multicast destination sends its first data packet piggybacked in a Mesh Request (MR) packet that is flooded up to a horizon threshold. If the interest expressed by the source spans more than the single data packet, the intended receiver(s) of a MR will establish and maintain a routing mesh spanning the active sources and the destination (a single node in the case of unicast and a set of nodes in the case of multicast). In the case of a multicast flow, the receivers of the multicast group run a distributed election using Mesh Announcement (MA) packets to elect a core for the group, which is the only receiver that continues to generate MAs for the group. No such election is needed for a unicast destination. An elected core or unicast destination continues sending MAs with monotonically increasing sequence numbers for as long as there is at least one active source interested in it. When no active sources are detected for a flow, the destination or core of the flow stops generating MAs, which causes the routing information corresponding to the mesh of the flow to be deleted. To save bandwidth, MAs for different unicast and multicast flows are grouped opportunistically in signaling packets. Furthermore, to confine control traffic to those portions of the network that need the information, an enclave (or region of interest) is defined for an established mesh. The enclave of a flow is a connected component of the network spanning all the receivers and sources of the flow and the relay nodes needed to connect them. The frequency with which MAs for a given flow are sent within an enclave is much higher than the frequency with which MAs are sent for a flow outside it, and depending on the flow type (e.g., bidirectional unicast or multicast) MAs are not propagated outside enclaves.

We compared the performance of PRIME against traditional routing protocols for unicast and multicast routing in MANETs using simulation experiments. Our comparison addressed the performance of the protocols purely for multicast routing, and their performance in supporting unicast and multicast routing. We compared PRIME with ODMRP to determine PRIME's effectiveness as just a multicast routing protocol, and consider different numbers of sources, groups, node densities and the use of group and random waypoint mobility models. We also compared PRIME against the use of AODV and ODMRP, and the use of OLSR and ODMRP. The results show that PRIME is a very efficient multicast routing protocol and provides substantial performance improvements over the traditional approach to supporting unicast and multicast routing. The results of our simulation experiments show that PRIME attains similar or better delivery ratios and significantly lower delays and communication overhead than the traditional approaches.

End-to-End Approach to Secure Routing in MANETs

Many security solutions have been proposed for routing protocols in mobile ad hoc networks (MANET); however, a complete and efficient solution to secure routing in MANETs has not yet been attained. We argue that this is due to the interplay between signaling packets and data packets, as well as the dynamic nature of MANETs. On-demand or proactive routing protocols based on the distributed computation of distances to destinations must disseminate signaling packets in which the routing metric to destinations is modified on a hop-by-hop basis, so that nodes order themselves with respect to destinations according to the routing metric (e.g., hop count). This empowers adversaries in a MANET to perform attacks by using false distance information to disrupt the ordering nodes try to establish for different destinations. This is especially problematic when nodes act in collusion with other nodes. Because of the problems in securing distance-based routing protocols, most previous approaches to secure routing in MANETs have focused on securing entire paths from source to destination or have each node along the path secure the link it intends to use. However, this is not a viable approach for large MANETs, because it leads to unsustainable flooding of control packets in a MANET. While the use of cryptography has been used to successfully counter many types of attacks, the solutions proposed to date do not guarantee that data packets are delivered, even if nodes comply with correct control signaling. In fact, many attacks are aimed at forcing data to be routed through adversary nodes, and once this is done they can perform denial of service, or disclosure attacks. It is possible that data can be routed, without any manipulation of the network, through adversaries and most previous work would provide no defense in this case. Such attacks can be best detected, and arguably can only be detected by end-to-end means. If these attacks were to occur when the known topology information is correct, then the best means of defense is path diversity.

We developed the Secure Routing through Diversity and Verification protocol (SRDV) as a secured distance vector protocol based on multipath routing. The goal of SRDV is to efficiently compute and use the shortest un-compromised paths available for the transmission of data through a network. SRDV accomplishes this by computing paths on-demand, ensuring the correctness and freshness of signaling through the use of digital signatures, sequence numbers, and hash chain authentication, verifying the performance of these paths with end-to-end probing to detect compromised paths, and load-balancing over a diverse set of paths (the region of interest) to counter attacks once detected. SRDV accomplishes this while using comparable, if not less, overhead than many traditional unsecured approaches. Our simulation results also show that the countermeasures employed in SRDV allows successful routing in the face of various attacks.

Time-Based Ordering

We developed a radically new approach to the ordering of nodes in a computer network that is based solely on the relative times when nodes transmit and receive signaling packets. We advocate the use of this time-based ordering as an alternative to the spatial orderings currently used in routing protocols. We prove the loop-free conditions for ordering based on time and demonstrate that it can provide a better foundation for routing in MANETs, given that it can perform as well as, and even better than routing schemes based on spatial ordering.

Time-based ordering provides a number of advantages over traditional spatial orderings. With time-based ordering, nodes have some control over the orderings they attain by simply controlling the times when they retransmit signaling packets. This contrasts with schemes based on spatial ordering in which the resulting order is predetermined by the physical network topology, and in some cases by the characteristics and utilization of links. Time-based ordering can increase substantially the number of usable paths between a source and its destinations, and therefore provide more robust routing in the face of mobility. Because time is always increasing, the resulting protocol can use non-sequential identification numbers to ensure that packet duplicates are not forwarded. Such numbers can be drawn from a space that is significantly smaller than traditional the one required for sequence numbers used in many routing protocols today. More importantly, the identification numbers needed for time-based ordering are reset locally without ever causing routing loops. By contrast, the sequence numbers needed in many routing protocols today must be drawn from large sequence-number spaces and aged out periodically (and hence require periodic transmissions by the origin of updates based on sequence numbers), and must incur network-wide overhead to be reset to prevent routing errors and loops.

We introduced the Time Ordered Routing Protocol (TORP) as an example of routing in wireless networks using time-based ordering. Results of simulation experiments show that TORP outperforms traditional routing protocols based on spatial ordering (OLSR, AODV, DYMO). In the simulation experiments, the load and mobility of the network were varied, and the results show great promise for time-based ordering. What is even more impressive is that this improvement does not come at the cost of overhead or delay. In fact, TORP incurred less than half the overhead of AODV, DYMO and OLSR in all scenarios. End-to-end delays and packet-delivery rates attained with TORP were much better than with the other routing protocols; while end-to-end delays with AODV were slightly better than with TORP, AODV delivered far fewer packets.

Sprout: Routing amid colluding attackers in multi-hop wireless networks

Routing protocols are subject to a wide variety of attacks, many of which can be highly disruptive. Many sophisticated attacks are ``insider attacks", in which the attacker has access to legitimate nodes or certain cryptographic credentials. Attacks by independent insiders have been addressed in the literature. However, much of the previous work focuses on providing a secure environment for ``insider" nodes with respect to attacking ``outsiders". Current secure routing protocols rarely address attacks by multiple colluding insiders. The problem becomes more pronounced in open networks, where nodes are considered legitimate members by default. Previous work on probabilistic routing focuses on selfish routing, and does not directly address routing security.

We propose Secure Probabilistic Routing (Sprout), a practical solution to the long-standing problem of secure wireless routing in the presence of multiple colluding ``insider" attackers. Sprout effectively mitigates the vast majority of the known routing layer attacks, and provides good performance in benign conditions. Sprout is a source-routed, link-state, multi-path routing protocol. In contrast with previous work, Sprout generates routes probabilistically, focusing in the first stage on diversity, rather than predicted performance. This makes it more resilient than previously proposed routing algorithms, to a wide variety of attacks. The obvious drawback of this approach is that many of the generated paths are of poor quality, and may include attackers. To address this, a performance based path selection algorithm is used as a second stage, which assigns a probability to each generated route depending on its measured reliability and end-to-end delay. Reliable routes with short round-trip times carry the majority of packets, while a fraction of packets are sent along other routes, to maintain diversity. With every new route sampled, the probability of finding a good one increases rapidly.

We have implemented Sprout in Linux, and deployed it on our 31-node indoor wireless testbed. Our extensive experimentation demonstrates the real-world performance of Sprout in terms of packet delivery ratio, round-trip times and TCP throughput. We evaluate Sprout performance in attack scenarios as well as in benign conditions. All tested attacks have marginal effect on Sprout. In comparing Sprout to shortest-path routing, we note that while Sprout is competitive in benign conditions, it also delivers consistently high, reliable performance in hostile environments. We present sample results below to demonstrate the effectiveness of Sprout.

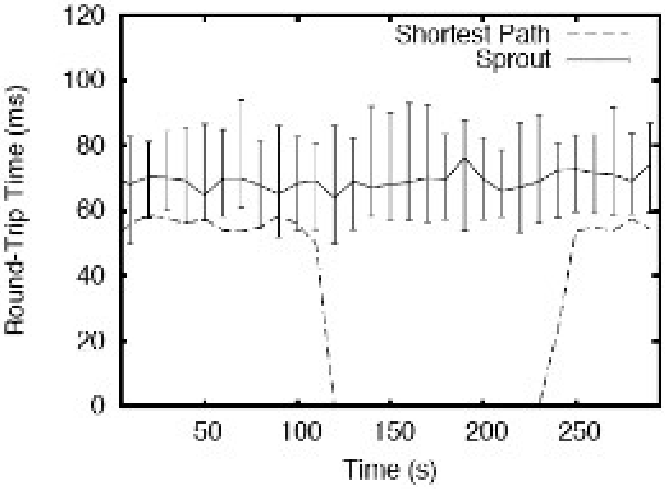


Fig 28. Sprout is effective against the black hole attack

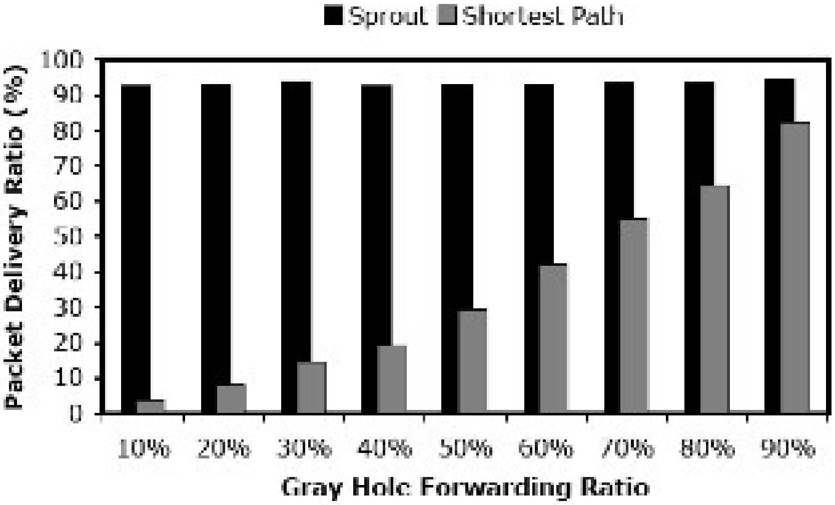


Fig 29. Sprout is effective against the Gray Hole attack

In the above figures we show the impact of an attacker that launches a black hole or a gray hole attack. The shortest path routing strategy is especially vulnerable to such attacks. However, we see that with Sprout, the impact of the attack is largely negated. In our paper, we also describe why Sprout is effective against a large class of other attacks.

6. Other Cross-Layer Aspects of MANET Security:

The accuracy of information regarding the state of the network is critical for insuring physical-layer information security. Specifically, the network state information can be divided into two broad categories: the quality of the wireless channels between users; and the capabilities of malicious users with regard to their antenna array size, jamming power, and attack strategies. Therefore, this thrust area focused on designing robust and secure transmission schemes for multi-antenna (MIMO) networks with imperfectly known channel state information (CSI). A second area of interest was the strategic interaction between legitimate network entities and malicious adversaries, and the resulting optimal countermeasures that provide a guaranteed level of security.

Although some research has been conducted on countering jamming attacks, few works consider jamming by insiders. Insider jammers are hard to deal with since they have all the group key information of other normal nodes. Due to physical limits on channel switching, there is limit on what an insider jammer can do, which creates an opportunity to develop our split and pairing solution.

To the best of our knowledge, no prior work has studied the Network partition problem due to the recurrence of primary users. Our solution is based on robust channel assignment, whereas prior channel assignment strategies only consider how to minimize the channel interference and thus the performance degrades substantially when the network partition occurs.

Secret key establishment based on channel information avoids the complexities of typical key generation exchanges. More importantly, key generation typically involves computation from a pseudo-random number generator, and therefore an attacker can more easily obtain the secret key if she can obtain some information about the number generator used. Because the physics of the multipath radio channel leads to complex numbers at different points in space that are, at least to an observer, truly random, basing the key on such physics avoids prior security vulnerabilities. However, accomplishing this key generation in practical systems requires that we establish efficient algorithms that can accurately estimate the channels and use them efficiently for key generation. It further requires that we be able to compensate for the non-reciprocal nature of the radio electronics that are included in the overall channel response.

Authentication using the non-ideal characteristics of each transmitter allows an additional layer of identification security that can help keep attackers from entering into a private data exchange. Furthermore, our work shows that using multiple antennas dramatically increases the reliability of this authentication. The challenge with this approach, however, is determining which set of all possible transmitter parameters should be measured. Furthermore, while it is relatively straightforward to identify a device when using very specialized measurement hardware (such as a vector signal analyzer), it becomes more difficult when the simpler hardware in each node must be able to perform measurements that can be used for accurate device identification.

Approaches proposed by researchers for secure device pairing, fall into two categories: (1) based on out-of-band channels, and (2) based on proximity. The existing solutions based on out-of-band channels require either sensors — such as cameras, microphones, or accelerometers – or peripherals, such as displays or keyboards. As wireless capability is expanding to a wide variety of devices (such as cameras, scanners, or even digital picture frames) that do not have these sensors or peripherals, the scope of applicability of these schemes is limited.

Wireless networks are susceptible to various types of attacks due to the “open air” nature of the wireless medium. Identity-based attacks (IBAs) are one of the most serious threats to wireless networks, and they are easy to launch. For instance, in IEEE 802.11 networks, an attacker can sniff the traffic in the network and get to know the MAC addresses of the legitimate users, and then masquerade as a legitimate user by modifying its own MAC address simply using an *ifconfig* command. IBAs are considered to be an important first step in an intruder’s attempt to launch a variety of other attacks on 802.11 networks, such as session hijacking, man-in-themiddle, data modification, and authentication-based denial of service.

Certain IBAs, such as deauthentication/disassociation attacks, are feasible mainly due to the fact that management and control frames are not protected in 802.11 networks. Although IEEE 802.11w adds protection to the management frames, it fails to protect against DoS attacks that are equivalent to the deauthentication and disassociation attacks. Furthermore, even with cryptographic mechanisms, the authentication key can still be compromised. If the key is broken, the cryptography-based mechanism will fail and IBAs are still possible.

Under the above circumstances, there is an increasing interest in using the physical-layer information or characteristics to detect IBAs in wireless networks. Received signal strength (RSS) information has been used for IBA detection due to its location distinction property and availability in the network interface card (NIC) of the off-the-shelf devices. RSS profiles are location specific and can be used to flag IBAs in static environments. Although the existing IBA detection schemes work well in a static network, they tend to raise excessive false alarms in a mobile environment where the RSS profiles change over time due to node mobility. *Although mobility is an inherent property of wireless networks, little work has addressed IBAs in mobile scenarios.*

While there have been several models for MIMO, we show that none of these models in fact represent the performance that one observes on real systems. Thus, this work tries to build models that are representative of what happens in real deployments.

In previous research on cooperative jamming in relay networks, there are some limitations, such as: 1) only single data stream transmission is considered, 2) the eavesdropper is only able to wiretap one hop of the relay transmission, 3) perfect CSI of the eavesdropper is available. This motivates us to examine a more general case of this topic.

In the case of single data stream cooperative jamming, the closed-form expression of the jamming beamformers contains the power parameter, which requires a complicated joint optimization for both the jamming beamformer and the power allocation. For the case of cooperative jamming using GSVD, the expression for the secrecy rate is complicated and difficult to implement power allocation even with geometric programming. In the cooperative jamming scheme for the case of unknown eavesdropper's CSI, the difficulty is how to achieve a tradeoff between power and allocation of the jamming subspace dimension.

Most of the previous research on cooperative jamming assumes that the eavesdropper's channel is perfectly known at the transmitters; however, this assumption is often not practical since malicious nodes may be passive and hide their presence. Therefore, the robust transmit design in our research will provide a more practical solution to the security concern in wireless networks.

The maximization of the secrecy rate is in general a non-convex problem, since it is the difference of two concave logarithm functions. In this project, since we consider secrecy rate based on the worst-case optimization, we bring an extra inner minimization inside the non-convex maximization problem. This makes the problem more difficult. Furthermore, we also consider the power allocation between the source and the friendly jammer. Thus a complicated joint optimization for both the transmit covariance matrices and the power allocation is required.

While secrecy capacity for the single-user wiretap channel with multi-antenna nodes has been extensively investigated, the effect of multi-antenna nodes on secrecy in multi-user scenarios has received little attention. Considering the problem from a game theoretic perspective, with transmitters as players, secrecy rates as utility functions, and transmission parameters as the game strategies, is another interesting topic.

Imperfect knowledge of CSI can arise due to numerous reasons such as user mobility, erroneous feedback, and harsh radio environments. The challenge is to devise a robust secure transmission scheme that is also general enough to encompass all such factors. While game-theoretic approaches to physical-layer security have slowly gained traction in the past two years, no prior work existed on framing the secrecy rate as a game payoff function. Therefore, we must first develop tractable expressions for the payoff function, and then examine the properties of the resulting secrecy game.

We showed that simple cooperative beamforming schemes can considerably improve the overall secrecy performance of the network compared with techniques where transmitters do not cooperate. Moreover, for the wiretap channel with an external jammer, where non-carefully designed jamming strategies can preclude secure communication, we obtained a jamming strategy that guarantees very good secrecy rate performance, even when there is no non-trivial null space between the helper and the intended receiver.

A naïve application of the secure beamforming scheme that wrongly assumes perfect CSI can significantly degrade the secrecy of the network and eliminate any expected benefits of the artificial jamming strategy, which then motivates the need to design a robust transmission scheme for the imperfect CSI scenario. The dual-mode eavesdropper/jammer model for the adversary has not been studied previously in the literature, which motivates the need to take a new approach towards the design of optimal countermeasures that ensure communications that are simultaneously reliable and secure.