MANET (Mobile Ad-hoc Networks)

1. A Novel Approach for Efficient Usage of Intrusion Detection System in Mobile Ad Hoc Networks
2. D2D: Delay-Aware Distributed Dynamic Adaptation of Contention Window in Wireless Networks
3. Detecting Colluding Blackhole and Greyhole Attacks in Delay Tolerant Networks
4. Distance-Based Location Management Utilizing Initial Position for Mobile Communication Networks
5. Mitigating Denial of Service Attacks in OLSR Protocol Using Fictitious Nodes
6. Opportunistic Routing With Congestion Diversity in Wireless Ad Hoc Networks
7. Top-k Query Processing and Malicious Node Identification Based on Node Grouping in MANETs
8. Resisting Black hole Attacks on MANET

WSN – Wireless Sensor Networks (Routing)


3. Cluster-Based Routing for the Mobile Sink in Wireless Sensor Networks With Obstacles

4. Code-Based Neighbor Discovery Protocols in Mobile Wireless Networks


7. Distributed Emergency Guiding with Evacuation Time Optimization Based on Wireless Sensor Networks

8. Duplicate Detectable Opportunistic Forwarding in Duty-Cycled Wireless Sensor Networks

9. Fair Routing for Overlapped Cooperative Heterogeneous Wireless Sensor Networks

10. Geographic and Opportunistic Routing for Underwater Sensor Networks

11. iPath: Path Inference in Wireless Sensor Networks

13. Location aware sensor routing protocol for mobile wireless sensor networks

14. Maximizing Data Collection Throughput on a Path in Energy Harvesting Sensor Networks Using a Mobile Sink

15. Maximum Data Collection Rate in Rechargeable Wireless Sensor Networks with Multiple Sinks


18. Privacy-Preserving Data Aggregation in Mobile Phone Sensing

19. RSSI-based Localization through Uncertain Data Mapping for Wireless Sensor Networks


**WSN – Wireless Sensor Networks (Security)**
1. A Secure and Efficient ID-Based Aggregate Signature Scheme for Wireless Sensor Networks

2. Active Trust: Secure and Trustable Routing in Wireless Sensor Networks


4. Analysis of One-Time Random Projections for Privacy Preserving Compressed Sensing

5. Energy and Memory Efficient Clone Detection in Wireless Sensor Networks

6. PKC-Based DoS Attacks-Resistant Scheme in Wireless Sensor Networks

7. Reliable and Efficient Data Acquisition in Wireless Sensor Networks in the Presence of Transfaulty Nodes

8. Traffic Decorrelation Techniques for Countering a Global Eavesdropper in WSNs

**VANET – Vehicular Ad-hoc Networks**

1. A Pseudonym Management System to Achieve Anonymity in Vehicular Ad Hoc Networks

2. A Threshold Anonymous Authentication Protocol for VANETs

3. ART: An Attack-Resistant Trust Management Scheme for Securing Vehicular Ad Hoc Networks
4. Coalition Formation for Cooperative Service-Based Message Sharing in Vehicular Ad Hoc Networks

5. Contact-Aware Data Replication in Roadside Unit Aided Vehicular Delay Tolerant Networks

6. DIVERT: A Distributed Vehicular Traffic Re-routing System for Congestion Avoidance

7. Dual Authentication and Key Management Techniques for Secure Data Transmission in Vehicular Ad Hoc Networks

8. LORA: Loss Differentiation Rate Adaptation Scheme for Vehicle-to-Vehicle Safety Communications

9. SCRP: Stable CDS-Based Routing Protocol for Urban Vehicular Ad Hoc Networks

10. Secure and Robust Multi-Constrained QoS Aware Routing Algorithm for VANETs

**WIRELESS COMMUNICATIONS**

1. A Hop-by-Hop Routing Mechanism for Green Internet

3. Assessing Performance Gains Through Global Resource Control of Heterogeneous Wireless Networks

4. Contact Duration Aware Data Replication in DTNs with Licensed and Unlicensed Spectrum

5. Cost-Aware Caching: Caching More (Costly Items) for Less (ISPs Operational Expenditures)


7. DSearching: Using Floating Mobility Information for Distributed Node Searching in DTNs

8. Dynamic Network Control for Confidential Multi-Hop Communications


10. Ghost-in-ZigBee: Energy Depletion Attack on ZigBee based Wireless Networks

11. Improving Access Point Association Protocols Through Channel Utilization and Adaptive Probing

12. LAAEM: A Method to Enhance LDoS Attack

13. Mimicry Attacks Against Wireless Link Signature and New Defense Using Time-Synched Link Signature
14. PROVEST: Provenance-based Trust Model for Delay Tolerant Networks

15. Routing Protocol for Heterogeneous Wireless Mesh Networks

16. Opportunistic Piggyback Marking for IP Traceback

17. Secure Transmission Against Pilot Spoofing Attack: A Two-Way Training-Based Scheme

18. Security Analysis and Improvements on Two Homomorphic Authentication Schemes for Network Coding

19. Thwarting Selfish Behavior in 802.11 WLANs

20. Mobility Prediction Based Joint Stable Routing and Channel Assignment for Mobile Ad Hoc Cognitive Networks


22. Local Anchor Schemes for Seamless and Low-Cost Handover in Coordinated Small Cells

23. Robotic Message Ferrying for Wireless Networks using Coarse-Grained Backpressure Control

24. TCP-Aware Backpressure Routing and Scheduling

25. Virtual Multipath Attack and Defense for Location Distinction in Wireless Networks