1. Record Nr. UNINA990009647080403321

Titolo	Groups and model theory : in honor of Rüdiger Göbel's 70th birthday, May 30-June 3, 2011, conference center "Die Wolfsburg", Mühlheim an der Ruhr, Germany / Luz Strüngmann, Manfred Droste, László Fuchs, Katrin Tent, editors
Pubbl/distr/stampa	Providence : American Mathematical Society, 2012
ISBN	978-0-8218-6923-9
Descrizione fisica	XVII, 316 p. ; 26 cm
Collana	Contemporary mathematics ; 576
Disciplina	512'.2
Locazione	MA1
Collocazione	C-1-(576 123-N-32
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia

2. Record Nr. UNINA9910955382503321

Titolo	From problem toward solution : wireless sensor networks security / / Zhen Jiang and Yi Pan, editors
Pubbl/distr/stampa	New York, : Nova Science Publishers, c2009
ISBN	1-61209-732-4
Edizione	[1st ed.]
Descrizione fisica	1 online resource (398 p.)
Collana	Distributed, cluster and grid computing
Altri autori (Persone)	JiangZhen PanYi <1960->
Disciplina	681/.25
Soggetti	Sensor networks - Security measures Wireless LANs - Security measures Wireless metropolitan area networks - Security measures Ad hoc networks (Computer networks) - Security measures
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Description based upon print version of record.
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Intro -- FROM PROBLEM TOWARD SOLUTION:WIRELESS SENSOR NETWORKSSECURITY -- Distributed, Cluster and Grid Computing -- FROM PROBLEM TOWARD SOLUTION:WIRELESS SENSOR NETWORKSSECURITY -- CONTENTS -- PREFACE -- PART 1.ATTACKS AND COUNTERMEASURES -- PRESERVING DATA AUTHENTICITY IN WIRELESSSENSOR NETWORKS: ATTACKS ANDCOUNTERMEASURES -- Abstract -- 1. Introduction -- 2. Models and Approaches -- 2.1. System Model -- 2.2. Threat Model -- 2.3. Solution Approaches -- 3. Passive Approaches -- 3.1. Secure Report Generation -- 3.2. Filtering with Uniform Key Sharing -- 3.3. Filtering with Route-specific Key Sharing -- 3.3.1. Interleaved Hop-by-hop Authentication -- 3.3.2. Other Solutions with Route-specific Key Sharing -- 3.4. Filtering with Location-based Key Sharing -- 3.4.1. Location-Based Resilient Security -- 3.4.2. Location-aware End-to-End Data Security -- 4. Proactive Approaches -- 4.1. Group Re-keying -- 4.2. Packet Traceback -- 4.3. Correlation among Data Content -- 4.3.1. Correlation Analysis and Modified t-test -- 5. Conclusion -- References -- LOCATION TRACKING ATTACK IN AD HOCNETWORKS BASED ON TOPOLOGY INFORMATION -- Abstract -- 1. Introduction -- 2. RelatedWork -- 3.

Localization Using Geometric Constraints -- 3.1. Constraint Solving Definitions -- 3.2. The Localization Algorithm -- 3.2.1. Phase 1-Deterministic Constraint Solving -- 3.2.2. Phase 2-Constraint Relaxation and Heuristic Improvements -- 3.3. Experimental Results -- 4. Localization Using DSR Protocol Information -- 4.1. Dynamic Source Routing -- 4.2. Scenario and Assumptions -- 4.3. Localization Approach -- 4.3.1. "Hop to Route Length Ratio" (HL) Heuristics -- 4.3.2. Derivation of Node Distribution along the Route from the HL Metric -- 4.3.3. Probability Based Position Estimation -- 4.4. Analysis -- 5. Conclusion -- Acknowledgement -- References.
PREVENTION OF DOS ATTACK IN SENSORNETWORKS USING REPEATED GAME THEORY -- Abstract -- 1. Introduction -- 2. RelatedWork -- 3. Game Formulation of the Proposed Protocol -- 3.1. Equilibrium -- 3.2. Payoff and Reputation -- 3.3. Protocol Description -- 4. Performance Evaluation -- 4.1. Metrics -- 4.2. Implementation -- References -- IMPACT OF PACKET INJECTION MODELSON MISBEHAVIOR DETECTION PERFORMANCEIN WIRELESS SENSOR NETWORKS -- Abstract -- 1. Introduction -- 1.1. Wireless Ad-Hoc Networks and the Concept of Misbehavior -- 1.2. Overview on Misbehavior in Wireless Ad-Hoc Networks -- 1.3. Intrusion Detection Systems - Detecting Misbehavior -- 1.4. Human Immune System - Inspiration for AIS -- 1.4.1. Adaptive Immune System -- 1.4.2. Innate Immune System -- 1.5. Translating Features of the HIS to AIS -- 2. Packet Injection Experiment - Problem Statement -- 2.1. Experimental Setup -- 2.2. Scenario Description -- 2.3. Network Topology -- 2.4. Node Misbehavior -- 2.5. Artificial Immune System - Details -- 3. Packet Injection Experiment - Results -- 4. AIS in Ad-Hoc Networks - RelatedWork -- 5. Conclusions and FutureWork -- Acknowledgments -- References -- PART 2.SECURED ROUTING AND LOCALIZATION -- SECURITY AWARE ROUTING IN HIERARCHICALOPTICAL SENSOR NETWORKS -- Abstract -- 1. Introduction -- 1.1. Motivation for Directional Optical Sensor Networks and Challenges -- 2. RelatedWork -- 3. Cluster-Based Directional Sensor Networks -- 3.1. Assumptions and Security Threat Model -- 4. The Security-Aware Base Station Circuit-Based Routing forCluster-based DOSN -- 4.1. Secure Neighborhood Discovery Protocol -- 5. Security Analysis -- 5.1. Per Hop Authentication and Alteration of Routing Beacons -- 5.2. Broadcast Authentication and Spoofed Routing Beacons -- 5.3. Beacon Freshness -- 6. Conclusion -- References -- SECURE MULTI-PATH DATA DELIVERY IN SENSORNETWORKS. Abstract -- 1. Introduction -- 2. System Models -- 2.1. Network Model -- 2.2. Attack Model -- 3. Node-disjoint Multi-path Encoding/Decoding -- 3.1. Multi-path Source Routing Encoding -- 3.2. Multi-path Data Encoding -- 3.3. Multi-path Data Decoding -- 3.4. Communication Overhead -- 4. Path Selection -- 4.1. v(3)-node-disjoint Shortest Paths -- 4.2. Path Rating Algorithm -- 4.3. Path Selection Algorithm -- 5. Robustness Analysis -- 5.1. General Evaluation Formulas -- 5.2. Uniform Block Allocation and Uniform Success Probability Distribution -- 5.3. Evaluate Success Probability for Multi-path Routing -- 6. Conclusion -- Appendices -- A. Encoding of Reed-Solomon Codes -- B. Decoding of Reed-Solomon Codes -- C. Proof of (21) -- References -- SELOC: SECURE LOCALIZATION FOR WIRELESSSENSOR AND ACTOR NETWORK -- Abstract -- 1. Introduction -- 2. RelatedWork -- 3. Network Model -- 3.1. Attack Models -- 3.2. Features of Secure Localization -- 4. SeLoc Secure Scheme -- 4.1. Brief Review of SeLoc Scheme -- 4.2. SeLoc Scheme -- 4.3. Location Verification -- 5. Security Analysis -- 5.1. Robustness -- 5.2. Sensitivity of SeLoc Scheme -- 6. Conclusion -- References -- PART 3. CRYPTOGRAPHY AND ENCRYPTION -- SECURITY IN WIRELESS SENSOR

NETWORKS:A FORMAL APPROACH -- Abstract -- 1. Introduction -- 2. Model Checking for the Analysis of Security Protocols -- 3. Sensor Network Encryption Protocol: SNEP -- 4. Verification of SNEP -- 5. RelatedWork -- Security Network Protocols -- Simulators of Sensor Networks -- Analysis with Model Checking Techniques -- 6. Conclusion -- References -- C4W: AN ENERGY EFFICIENT PUBLIC KEYCRYPTOSYSTEM FOR LARGE-SCALE WIRELESSSENSOR NETWORKS -- Abstract -- 1. Introduction -- 1.1. Related Work -- 1.2. Contributions -- 2. Combined Public Key Scheme for Wireless Sensor Networks -- 2.1. Basic Scheme -- 2.2. Security-Enhanced Scheme (SES). 2.3. Protocol -- 3. Analysis -- 3.1. Security -- 3.2. Energy -- 4. Conclusion -- References -- ENERGY CONSUMPTION OF SECURITY ALGORITHMSIN WIRELESS SENSOR NODES -- Abstract -- 1. Introduction -- 2. Cryptographic Algorithms for WSN Nodes -- 2.1. New Method for Reorganization of Cryptographic Algorithms -- 2.2. Related Work -- 2.3. Verification of Results -- 3. Measurement of Energy Consumption for Security -- 3.1. Tradeoff between Security and Energy Consumption -- 3.2. Related Work -- 3.3. Measurement Techniques -- 3.4. Energy Consumption without Security -- 3.4.1. Measurements for CrossBow Nodes -- 3.4.2. Measurements for Ember Nodes -- 3.5. Energy Consumption for Security -- 3.5.1. Energy Consumption for Security in CrossBow Nodes -- 3.5.2. Energy Consumption for Security in Ember Nodes -- 3.5.3. Comparisons of CrossBow &amp -- Ember Nodes -- 4. Assessment of Life-Time Energy Consumption -- 4.1. Life Time Energy Consumption -- 4.2. Energy Measurements and Profile Analyzer -- 4.2.1. Operational Circuit -- 4.2.2. Measurement Record Program -- 4.2.3. E-Analyzer: Energy Profile Analyzer -- 4.3. Case Study: Security Algorithms in CrossBow MICA2 Nodes -- 5. Guidelines to Apply Security into WSN -- 6. Conclusions -- References -- PART 4.KEY PRE-DISTRIBUTION AND REVOCATION -- DETERMINISTIC AND RANDOMIZED KEYPRE-DISTRIBUTION SCHEMES FOR MOBILEAD-HOC NETWORKS: FOUNDATIONS ANDEXAMPLE CONSTRUCTIONS -- Abstract -- 1. Introduction -- 2. General Considerations for Key Management Schemes -- 3. Techniques -- 3.1. Random Graph Based -- 4. Set System Based -- 4.0.1. Constrained Intersection Matrices -- 4.0.2. The BBR Polynomials -- 5. RandomWalk Based -- 5.1. Approximating the Evolution of Stochastic Processes -- 5.2. Gradual Increase of the Bit-Correlation -- 5.3. The General k-place Elimination Protocol -- 5.4. Assessment of the Elimination Protocol.
6. Probabilistic Technique Based -- 7. Conclusions -- References -- ARPD: ASYNCHRONOUS RANDOM KEYPREDISTRIBUTION IN THE LEAP FRAMEWORKFOR WIRELESS SENSOR NETWORKS -- Abstract -- 1. Introduction -- 2. RelatedWork -- 2.1. Pairwise Key Establishment in LEAP -- 2.1.1. LEAP Security -- 2.2. Random Pairwise Key Predistribution -- 3. ARPD for Node Additions -- 4. Performance Analysis -- 4.1. Section Notation and Assumptions -- 4.2. Probability of Connectivity -- 4.2.1. Key Reuse -- 4.2.2. Choice of Reuse Factor -- 5. Security Analysis -- 5.1. A Security Threat Model for WSNs -- 5.2. Outside Attacks -- 5.3. Inside Attacks -- 6. Conclusions -- References -- SECURE k-CONNECTIVITY PROPERTIESOF WIRELESS SENSOR NETWORKS -- Abstract -- 1. Introduction -- 2. The Reference Model -- 3. k-Connectivity of Kryptographs -- 3.1. Survivor Function Pr {connectivity k} -- 3.2. Expected Connectivity -- 4. Simulation Results -- 5. RelatedWork -- 6. Conclusion -- References -- GATEWAY SUBSET DIFFERENCE REVOCATION -- Abstract -- 1. Introduction -- 2. Subset Difference Revocation -- 3. Gateway Subset Difference Revocation -- 4. Evaluation -- 4.1. Security -- 4.2. Memory -- 4.3. Processing Load -- 5. Related Work -- 6. Conclusion -- References --

PART 5.KEY EXCHANGE AND ACCESS CONTROL -- AUTHENTICATED KEY EXCHANGE WITH GROUPSUPPORT FOR WIRELESS SENSOR NETWORKS -- Abstract -- 1. Introduction -- 1.1. Node-Compromise Attacker Model -- 1.2. Secure Link Communication -- 1.2.1. Random Key Pre-distribution -- 1.2.2. Pairwise Key Pre-distribution -- 1.3. Seed-Based Pre-distribution -- 1.3.1. Selective Node Capture Attack -- 1.3.2. Hypercube Pre-distribution -- 2. Group Supported Key Exchange -- 2.1. Authenticated Key Exchange with Group Support -- 2.2. Probabilistic Authentication -- 2.2.1. Probabilistic Authentication with Majority Decision.
2.3. Evaluation of the Communication and Computation Overhead.

Sommario/riassunto

Reserving data authenticity in a hostile environment, where the sensor nodes may be compromised is a critical security issue for wireless sensor networks. This book covers location tracking attack in ad hoc networks based on topolgy information, security aware routing in hierarchical optical sensor networks and more.