Secure Wireless Sensor Networks Problems And Solutions

Secure Wireless Sensor Networks-Mauro Conti 2015-11-06 This book explores five fundamental mechanisms to build secure Wireless Sensor Networks (WSNs). It presents security issues related to a single node which deals with the authentication and communication confidentiality with other nodes. It also focuses on network security, providing solutions for the node capture attack and the clone attack. It examines a number of areas and problems to which WSNs are applied continuously, including: supporting rescue operations, building surveillance, fire prevention, battlefield monitoring and more. However, known and unknown threats still affect WSNs and in many applications of this new technology the security of the network is a fundamental issue for confidentiality, integrity, authenticity and availability. The last section of the book addresses security for a common WSN service. Case studies are provided throughout. Secure Wireless Sensor Networks: Threats and Solutions targets advanced-level students and researchers in computer science and electrical engineering as a secondary text book. Professionals working in the wireless sensor networks field will also find this book useful as a reference.

Secure Localization and Time Synchronization for Wireless Sensor and Ad Hoc Networks-Radha Poovendran 2007-12-03 This book presents the latest research results in the area of secure localization for both wireless mobile ad hoc networks and wireless sensor networks. It is suitable as a text for computer science courses in wireless systems and security. It includes implementation studies with mica2 mote sensors. Due to the open
spectrum nature of wireless communication, it is subject to attacks and intrusions. Hence the wireless network synchronization needs to be both robust and secure. Furthermore, issues such as energy constraints and mobility make the localization process even more challenging. The book will also interest developers of secure wireless systems.

Secure Wireless Sensor Networks—Mauro Conti (Associate professor) 2015

This book explores five fundamental mechanisms to build secure Wireless Sensor Networks (WSNs). It presents security issues related to a single node which deals with the authentication and communication confidentiality with other nodes. It also focuses on network security, providing solutions for the node capture attack and the clone attack. It examines a number of areas and problems to which WSNs are applied continuously, including: supporting rescue operations, building surveillance, fire prevention, battlefield monitoring and more. However, known and unknown threats still affect WSNs and in many applications of this new technology the security of the network is a fundamental issue for confidentiality, integrity, authenticity and availability. The last section of the book addresses security for a common WSN service. Case studies are provided throughout. Secure Wireless Sensor Networks: Threats and Solutions targets advanced-level students and researchers in computer science and electrical engineering as a secondary textbook. Professionals working in the wireless sensor networks field will also find this book useful as a reference.

Security and Privacy Issues in IoT Devices and Sensor Networks—Sudhir Kumar Sharma 2020-10-23

Security and Privacy Issues in IoT Devices and Sensor Networks investigates security breach issues in IoT and sensor networks, exploring various solutions. The book follows a two-fold approach, first focusing on the fundamentals and theory surrounding sensor networks and IoT security. It then explores practical solutions that can be implemented to develop security for these elements, providing
case studies to enhance understanding. Machine learning techniques are covered, as well as other security paradigms, such as cloud security and cryptocurrency technologies. The book highlights how these techniques can be applied to identify attacks and vulnerabilities, preserve privacy, and enhance data security. This in-depth reference is ideal for industry professionals dealing with WSN and IoT systems who want to enhance the security of these systems. Additionally, researchers, material developers and technology specialists dealing with the multifarious aspects of data privacy and security enhancement will benefit from the book's comprehensive information. Provides insights into the latest research trends and theory in the field of sensor networks and IoT security Presents machine learning-based solutions for data security enhancement Discusses the challenges to implement various security techniques Informs on how analytics can be used in security and privacy

Wireless Sensor Network Security-Javier López 2008 Wireless sensor networks (WSN) is especially vulnerable against external and internal attacks due to its particular characteristics. This book provides an overview of the major security issues that various WSN designers have to face, and also gives a comprehensive guide of solutions and open problems.

Security in Wireless Sensor Networks-George S. Oreku 2015-09-12 This monograph covers different aspects of sensor network security including new emerging technologies. The authors present a mathematical approach to the topic and give numerous practical examples as well as case studies to illustrate the theory. The target audience primarily comprises experts and practitioners in the field of sensor network security, but the book may also be beneficial for researchers in academia as well as for graduate students.

Secure Wireless Sensor Networks introduces the reader to the fundamentals and key issues related to wireless ad hoc networking, with an emphasis on security. It discusses the security attacks and counter measures in wireless ad hoc, sensor and mesh networks, and briefly presents the standards on related topics. The authors offer a clear exposition of various challenges and solutions in this field including bootstrapping, key distribution and exchange, authentication issues, privacy, anonymity and tamper resilience. Key Features: Introduces the fundamentals and key issues of the new technologies followed by comprehensive presentation on security attacks and counter measures Covers Denial of Service (DoS) attacks, hardware aspects of secure wireless ad hoc and sensor networks and secure routing Contains information on cryptographic primitives and electronic warfare Includes problems at the end of each chapter to enhance learning. This book is well suited for graduate students in computer, electrical and communications engineering and computer science departments, researchers in academia and industry, as well as C4I engineers and officers in the military. Wireless network designers for internet service providers and mobile communications operators will also find this book very useful. Security for Wireless Sensor Networks using Identity-Based Cryptography-Harsh Kupwade Patil 2013-03-21 Security for Wireless Sensor Networks using Identity-Based Cryptography introduces identity-based cryptographic schemes for wireless sensor networks. It starts with an exhaustive survey of the existing layered approach to WSN security—detailing its pros and cons. Next, it examines new attack vectors that exploit the layered approach to security. After providing the necessary background, the book presents a cross-layer design approach that addresses authentication, integrity, and encryption. It also examines new ID-based key management mechanisms using a cross-layer design perspective. In addition, secure routing algorithms using ID-based cryptography are also discussed.
Supplying readers with the required foundation in elliptic curve cryptography and identity-based cryptography, the authors consider new ID-based security solutions to overcome cross layer attacks in WSN. Examining the latest implementations of ID-based cryptography on sensors, the book combines cross-layer design principles along with identity-based cryptography to provide you with a new set of security solutions that can boost storage, computation, and energy efficiency in your wireless sensor networks.

Next Generation Wireless Network Security and Privacy-Lakhtaria, Kamaljit I. 2015-10-13 As information resources migrate to the Cloud and to local and global networks, protecting sensitive data becomes ever more important. In the modern, globally-interconnected world, security and privacy are ubiquitous concerns. Next Generation Wireless Network Security and Privacy addresses real-world problems affecting the security of information communications in modern networks. With a focus on recent developments and solutions, as well as common weaknesses and threats, this book benefits academicians, advanced-level students, researchers, computer scientists, and software development specialists. This cutting-edge reference work features chapters on topics including UMTS security, procedural and architectural solutions, common security issues, and modern cryptographic algorithms, among others.

Secure Localization and Time Synchronization for Wireless Sensor and Ad Hoc Networks-Radha Poovendran 2006-11-14 This book presents the latest research results in the area of secure localization for both wireless mobile ad hoc networks and wireless sensor networks. It is suitable as a text for computer science courses in wireless systems and security. It includes implementation studies with mica2 mote sensors. Due to the open spectrum nature of wireless communication, it is subject to attacks and intrusions. Hence the wireless network synchronization needs to be both robust and secure.
Furthermore, issues such as energy constraints and mobility make the localization process even more challenging. The book will also interest developers of secure wireless systems.

Security in RFID and Sensor Networks-Paris Kitsos 2016-04-19 In the past several years, there has been an increasing trend in the use of Radio Frequency Identification (RFID) and Wireless Sensor Networks (WSNs) as well as in the integration of both systems due to their complementary nature, flexible combination, and the demand for ubiquitous computing. As always, adequate security remains one of the open areas of concern before wide deployment of RFID and WSNs can be achieved. Security in RFID and Sensor Networks is the first book to offer a comprehensive discussion on the security challenges and solutions in RFID, WSNs, and integrated RFID and WSNs, providing an essential reference for those who regularly interface with these versatile technologies.

Exposes Security Risks The book begins with a discussion of current security issues that threaten the effective use of RFID technology. The contributors examine multi-tag systems, relay attacks, authentication protocols, lightweight cryptography, and host of other topics related to RFID safety. The book then shifts the focus to WSNs, beginning with a background in sensor network security before moving on to survey intrusion detection, malicious node detection, jamming, and other issues of concern to WSNs and their myriad of applications.

Offers Viable Solutions In each chapter, the contributors propose effective solutions to the plethora of security challenges that confront users, offering practical examples to aid in intuitive understanding. The last part of the book reviews the security problems inherent in integrated RFID & WSNs. The book ends with a glimpse of the future possibilities in these burgeoning technologies and provides recommendations for the proactive design of secure wireless embedded systems.

explores various challenging problems and applications areas of wireless sensor networks (WSNs), and identifies the current issues and future research challenges. Discussing the latest developments and advances, it covers all aspects of in WSNs, from architecture to protocols design, and from algorithm development to synchronization issues. As such the book is an essential reference resource for undergraduate and postgraduate students as well as scholars and academics working in the field.

Security in Sensor Networks-Yang Xiao 2016-04-19 Sensor networks differ from traditional networks in many aspects including their limited energy, memory space, and computational capability. These differentiators create unique security vulnerabilities. Security in Sensor Networks covers all aspects of the subject, serving as an invaluable reference for researchers, educators, and practitioners.

Security for Wireless Sensor Networks-Donggang Liu 2007-02-15 This book discusses fundamental security issues in wireless sensor networks, techniques for the protection of such networks, as well as results from recent studies in wireless sensor network security. It contains example applications for target tracking, scientific exploration and data acquisition in hazardous environments, and includes a fairly new study on capabilities of mu-TESLA, a broadcast authentication technique for wireless sensor networks. The book assists both professionals and students to understand background knowledge in wireless sensor network security and prepare them for producing research in this domain.

Guide to Wireless Sensor Networks-Sudip Misra 2009-05-29 Overview and Goals Wireless communication technologies are undergoing rapid advancements. The last few years have experienced a steep growth in research in the area of wireless sensor networks (WSNs). In WSNs, communication takes place with the help of spatially distributed autonomous sensor node equipped to sense specific information.
ation. WSNs, especially the ones that have gained much popularity in the recent years, are, ty-
cally, ad hoc in nature and they inherit many characteristics/features of wireless ad hoc
networks such as the ability for infrastructure-less setup, minimal
or no reliance on network planning, and the ability of the nodes to
self-organize and self-con?gure without the involvement of a
centralized network manager, router, access point, or a switch.
These features help to set up WSNs fast in situations where there
is no existing network setup or in times when setting up a ?xed
infrastructure network is considered infeasible, for example, in
times of emergency or during relief - erations. WSNs ?nd a
variety of applications in both the military and the civilian
population worldwide such as in cases of enemy intrusion in the
battle?eld, object tracking, habitat monitoring, patient
monitoring, ?re detection, and so on. Even though sensor
networks have emerged to be attractive and they hold great
promises for our future, there are several challenges that need to
be addressed. Some of the well-known challenges are attributed
to issues relating to coverage and deployment, scalability, quality-
of-service, size, computational power, energy ef?ciency, and
security.
Proceeding of the International Conference on Computer
Networks, Big Data and IoT (ICCBI - 2019)-A. Pasumpon Pandian
2020-03-04 This book presents the proceedings of the
International Conference on Computing Networks, Big Data and
IoT [ICCBI 2019], held on December 19–20, 2019 at the Vaigai
College of Engineering, Madurai, India. Recent years have
witnessed the intertwining development of the Internet of Things
and big data, which are increasingly deployed in computer
network architecture. As society becomes smarter, it is critical to
replace the traditional technologies with modern ICT
architectures. In this context, the Internet of Things connects
smart objects through the Internet and as a result generates big
data. This has led to new computing facilities being developed to
derive intelligent decisions in the big data environment. The book covers a variety of topics, including information management, mobile computing and applications, emerging IoT applications, distributed communication networks, cloud computing, and healthcare big data. It also discusses security and privacy issues, network intrusion detection, cryptography, 5G/6G networks, social network analysis, artificial intelligence, human–machine interaction, smart home and smart city applications.

Wireless Sensor Networks-Rastko R. Selmic 2016-11-02
This book presents a comprehensive overview of wireless sensor networks (WSNs) with an emphasis on security, coverage, and localization. It offers a structural treatment of WSN building blocks including hardware and protocol architectures and also provides a systems-level view of how WSNs operate. These building blocks will allow readers to program specialized applications and conduct research in advanced topics. A brief introductory chapter covers common applications and communication protocols for WSNs. Next, the authors review basic mathematical models such as Voroni diagrams and Delaunay triangulations. Sensor principles, hardware structure, and medium access protocols are examined. Security challenges ranging from defense strategies to network robustness are explored, along with quality of service measures. Finally, this book discusses recent developments and future directions in WSN platforms. Each chapter concludes with classroom-tested exercises that reinforce key concepts. This book is suitable for researchers and for practitioners in industry. Advanced-level students in electrical engineering and computer science will also find the content helpful as a textbook or reference.

Fundamentals of Wireless Sensor Networks-Waltenegus Dargie 2010-11-05
In this book, the authors describe the fundamental concepts and practical aspects of wireless sensor networks. The book provides a comprehensive view to this rapidly evolving field, including its many novel applications, ranging from protecting...
civil infrastructure to pervasive health monitoring. Using detailed examples and illustrations, this book provides an inside track on the current state of the technology. The book is divided into three parts. In Part I, several node architectures, applications and operating systems are discussed. In Part II, the basic architectural frameworks, including the key building blocks required for constructing large-scale, energy-efficient sensor networks are presented. In Part III, the challenges and approaches pertaining to local and global management strategies are presented – this includes topics on power management, sensor node localization, time synchronization, and security. At the end of each chapter, the authors provide practical exercises to help students strengthen their grip on the subject. There are more than 200 exercises altogether. Key Features: Offers a comprehensive introduction to the theoretical and practical concepts pertaining to wireless sensor networks Explains the constraints and challenges of wireless sensor network design; and discusses the most promising solutions Provides an in-depth treatment of the most critical technologies for sensor network communications, power management, security, and programming Reviews the latest research results in sensor network design, and demonstrates how the individual components fit together to build complex sensing systems for a variety of application scenarios Includes an accompanying website containing solutions to exercises (http://www.wiley.com/go/dargie_fundamentals) This book serves as an introductory text to the field of wireless sensor networks at both graduate and advanced undergraduate level, but it will also appeal to researchers and practitioners wishing to learn about sensor network technologies and their application areas, including environmental monitoring, protection of civil infrastructure, health care, precision agriculture, traffic control, and homeland security.

Security in Ad Hoc and Sensor Networks-Raheem Beyah 2010

Security issues in ad hoc and sensor networks have become
extremely important. This edited book provides a comprehensive treatment for security issues in these networks, ranging from attack mitigation to recovery after an attack has been successfully executed. Security issues addressed include (but are not limited to) attacks, malicious node detection, access control, authentication, intrusion detection, privacy and anonymity, key management, location verification, security architectures and protocols, secrecy and integrity, network resilience and survivability, and trust models. This complete book provides an excellent reference for students, researchers, and industry practitioners related to these areas.

Security and Privacy Issues in Sensor Networks and IoT-Ahlawat, Priyanka 2019-10-25 As technology continues to expand and develop, the internet of things (IoT) is playing a progressive role in the infrastructure of electronics. The increasing amount of IoT devices, however, has led to the emergence of significant privacy and security challenges. Security and Privacy Issues in Sensor Networks and IoT is a collection of innovative research on the methods and applications of protection disputes in the internet of things and other computing structures. While highlighting topics that include cyber defense, digital forensics, and intrusion detection, this book is ideally designed for security analysts, IT specialists, software developers, computer engineers, industry professionals, academicians, students, and researchers seeking current research on defense concerns in cyber physical systems.

Algorithms and Protocols for Wireless Sensor Networks-Azzedine Boukerche 2008-11-03 A one-stop resource for the use of algorithms and protocols in wireless sensor networks From an established international researcher in the field, this edited volume provides readers with comprehensive coverage of the fundamental algorithms and protocols for wireless sensor networks. It identifies the research that needs to be conducted on a number of levels to design and assess the deployment of wireless sensor networks, and provides an in-depth analysis of the
development of the next generation of heterogeneous wireless sensor networks. Divided into nineteen succinct chapters, the book covers: mobility management and resource allocation algorithms; communication models; energy and power consumption algorithms; performance modeling and simulation; authentication and reputation mechanisms; algorithms for wireless sensor and mesh networks; and algorithm methods for pervasive and ubiquitous computing; among other topics. Complete with a set of challenging exercises, this book is a valuable resource for electrical engineers, computer engineers, network engineers, and computer science specialists. Useful for instructors and students alike, Algorithms and Protocols for Wireless Sensor Networks is an ideal textbook for advanced undergraduate and graduate courses in computer science, electrical engineering, and network engineering.

Underwater Acoustic Sensor Networks-Yang Xiao 2010-05-19 A detailed review of underwater channel characteristics, Underwater Acoustic Sensor Networks investigates the fundamental aspects of underwater communication. Prominent researchers from around the world consider contemporary challenges in the development of underwater acoustic sensor networks (UW-ASNs) and introduce a cross-layer approach for effective integration of all communication functionalities. Discussing architectures for two- and three-dimensional sensor networks, this authoritative resource clearly delineates the main differences between terrestrial and underwater sensor networks—covering the wide range of topics related to UW-ASNs. It examines efficient distributed routing algorithms for delay-insensitive and delay-sensitive applications and introduces a realistic acoustic model characterized by channel utilization efficiency that enables proper setting of the optimal packet size for underwater communication. It also: Provides efficient sensor communication protocols for the underwater environment Addresses the topology control problem for sparse and dense 3D
networks Presents a novel distributed MAC protocol that incorporates a unique closed-loop distributed algorithm for setting the optimal transmit power and code length. The book includes coverage of routing, fault tolerance, time synchronization, optimal clustering, medium access control, software, hardware, and channel modeling. Exploring the need to design an energy-efficient cross-layer protocol suite, this resource provides the understanding required to achieve high-performance channel access, routing, event transport reliability, and data flow control with underwater acoustic sensors.

Encyclopedia on Ad Hoc and Ubiquitous Computing—Dharma P. Agrawal 2010 Ad hoc and ubiquitous computing technologies have received extensive attention in both the academia and industry with the explosive growth of wireless communication devices. These technologies are beneficial for many applications, such as offering futuristic high-bandwidth access for users, and are expected to offer more exciting and efficient services, anytime and anywhere. In order to satisfy these diverse applications, the design issues of various wireless networks such as ad hoc, sensor, and mesh networks are extremely complicated and there are a number of technique challenges that need to be explored, involving every layer of the OSI protocol stack. This book aims to provide a complete understanding of these networks by investigating the evolution of ad hoc, sensor, and mesh networking technologies from theoretic concept to implementation protocols, from fundamentals to real applications. It provides the necessary background material needed to go deeper into the subject and explore the research literature. The explanation in the book is therefore sufficiently detailed to serve as a comprehensive reference for students, instructors, researchers, engineers, and other professionals, building their understanding of these networks.

Wireless sensor networks have gained significant attention industrially and academically due to their wide range of uses in various fields. Because of their vast amount of applications, wireless sensor networks are vulnerable to a variety of security attacks. The protection of wireless sensor networks remains a challenge due to their resource-constrained nature, which is why researchers have begun applying several branches of artificial intelligence to advance the security of these networks. Research is needed on the development of security practices in wireless sensor networks by using smart technologies.

**Deep Learning Strategies for Security Enhancement in Wireless Sensor Networks** provides emerging research exploring the theoretical and practical advancements of security protocols in wireless sensor networks using artificial intelligence-based techniques. Featuring coverage on a broad range of topics such as clustering protocols, intrusion detection, and energy harvesting, this book is ideally designed for researchers, developers, IT professionals, educators, policymakers, practitioners, scientists, theorists, engineers, academicians, and students seeking current research on integrating intelligent techniques into sensor networks for more reliable security practices.

Wireless Sensor Networks-Kazem Sohraby 2007-04-06
Infrastructure for Homeland Security Environments Wireless Sensor Networks helps readers discover the emerging field of low-cost standards-based sensors that promise a high order of spatial and temporal resolution and accuracy in an ever-increasing universe of applications. It shares the latest advances in science and engineering paving the way towards a large plethora of new applications in such areas as infrastructure protection and security, healthcare, energy, food safety, RFID,
ZigBee, and processing. Unlike other books on wireless sensor networks that focus on limited topics in the field, this book is a broad introduction that covers all the major technology, standards, and application topics. It contains everything readers need to know to enter this burgeoning field, including current applications and promising research and development; communication and networking protocols; middleware architecture for wireless sensor networks; and security and management. The straightforward and engaging writing style of this book makes even complex concepts and processes easy to follow and understand. In addition, it offers several features that help readers grasp the material and then apply their knowledge in designing their own wireless sensor network systems: * Examples illustrate how concepts are applied to the development and application of * wireless sensor networks * Detailed case studies set forth all the steps of design and implementation needed to solve real-world problems * Chapter conclusions that serve as an excellent review by stressing the chapter's key concepts * References in each chapter guide readers to in-depth discussions of individual topics This book is ideal for networking designers and engineers who want to fully exploit this new technology and for government employees who are concerned about homeland security. With its examples, it is appropriate for use as a coursebook for upper-level undergraduates and graduate students.

Security in Wireless Ad Hoc and Sensor Networks-Erdal Cayirci

This book provides an in-depth guide to security in wireless ad hoc and sensor networks. Security in Wireless Ad Hoc and Sensor Networks introduces the reader to the fundamentals and key issues related to wireless ad hoc networking, with an emphasis on security. It discusses the security attacks and counter measures in wireless ad hoc, sensor and mesh networks, and briefly presents the standards on related topics. The authors offer a clear exposition of various challenges and solutions in this.
field including bootstrapping, key distribution and exchange, authentication issues, privacy, anonymity and tamper resilience. Key Features: Introduces the fundamentals and key issues of the new technologies followed by comprehensive presentation on security attacks and counter measures Covers Denial of Service (DoS) attacks, hardware aspects of secure wireless ad hoc and sensor networks and secure routing Contains information on cryptographic primitives and electronic warfare Includes problems at the end of each chapter to enhance learning. This book is well suited for graduate students in computer, electrical and communications engineering and computer science departments, researchers in academia and industry, as well as C4I engineers and officers in the military. Wireless network designers for internet service providers and mobile communications operators will also find this book very useful.

ICCCE 2018-Amit Kumar 2018-08-31 This book comprises selected articles from the International Communications Conference (ICC) 2018 held in Hyderabad, India in 2018. It offers in-depth information on the latest developments in voice-, data-, image- and multimedia processing research and applications, and includes contributions from both academia and industry.


Architectural Wireless Networks Solutions and Security Issues-Santosh Kumar Das

Wireless Sensor Networks-Shafiullah Khan 2016-04-21 Wireless sensor networks (WSNs) utilize fast, cheap, and effective applications to imitate the human intelligence capability of sensing on a wider distributed scale. But acquiring data from the deployment area of a WSN is not always easy and multiple issues arise, including the limited resources of sensor devices run with one-time batteries. Additi

Wireless Sensor Networks-Jun Zheng 2009-10-27 Learn the fundamental concepts, major challenges, and effective solutions
in wireless sensor networking This book provides a comprehensive and systematic introduction to the fundamental concepts, major challenges, and effective solutions in wireless sensor networking (WSN). Distinguished from other books, it focuses on the networking aspects of WSNs and covers the most important networking issues, including network architecture design, medium access control, routing and data dissemination, node clustering, node localization, query processing, data aggregation, transport and quality of service, time synchronization, network security, and sensor network standards. With contributions from internationally renowned researchers, Wireless Sensor Networks expertly strikes a balance between fundamental concepts and state-of-the-art technologies, providing readers with unprecedented insights into WSNs from a networking perspective. It is essential reading for a broad audience, including academic researchers, research engineers, and practitioners in industry. It is also suitable as a textbook or supplementary reading for electrical engineering, computer engineering, and computer science courses at the graduate level. 2016 International Conference on Advances in Computing, Communication and Automation- 2016 Security of Self-Organizing Networks-Al-Sakib Khan Pathan 2016-04-19 Reflecting recent advancements, Security of Self-Organizing Networks: MANET, WSN, WMN, VANET explores wireless network security from all angles. It begins with a review of fundamental security topics and often-used terms to set the foundation for the following chapters. Examining critical security issues in a range of wireless networks, the book proposes specific solutions to security threats. Ideal for those with a basic understanding of network security, the text provides a clear examination of the key aspects of security in self-organizing networks and other networks that use wireless technology for communications. The book is organized into four sections for ease of reference: General Topics—Security of Wireless and Self-
Organizing Networks Mobile Ad-Hoc Network and Vehicular Ad-Hoc Network Security Wireless Sensor Network Security Wireless Mesh Network Security Highlighting potential threats to network security, most chapters are written in a tutorial manner. However, some of the chapters include mathematical equations and detailed analysis for advanced readers. Guiding you through the latest trends, issues, and advances in network security, the text includes questions and sample answers in each chapter to reinforce understanding.

Security and Privacy in Smart Sensor Networks-Maleh, Yassine 2018-05-09 Security and privacy protection within computer networks can be a challenge. By examining the current problems and challenges this domain is facing, more efficient strategies can be established to safeguard personal information against invasive pressures. Security and Privacy in Smart Sensor Networks is a critical scholarly resource that examines recent developments and emerging trends in smart sensor security and privacy by providing new models, practical solutions, and technological advances related to security. Featuring coverage on a broad range of topics such as cloud security, encryption, and intrusion detection systems, this book is geared towards academicians, engineers, IT specialists, researchers, and students seeking current research on authentication and intrusion detection.

Wireless Sensor Networks and Applications-Yingshu Li 2008-02-10 A crucial reference tool for the increasing number of scientists who depend upon sensor networks in a widening variety of ways. Coverage includes network design and modeling, network management, data management, security and applications. The topic covered in each chapter receives expository as well as scholarly treatment, covering its history, reviewing state-of-the-art thinking relative to the topic, and discussing currently unsolved problems of special interest.

From Problem Toward Solution-Zhen Jiang 2008-07-01 Reserving data authenticity in a hostile environment, where the sensor
nodes may be compromised, is a critical security issue for wireless sensor networks. In such networks, once a real event is detected, nearby sensors generate data reports which are subsequently forwarded to the data collection point. However, the subverted sensors, which have access to the stored secret keys, can launch attacks to compromise data authenticity. They can act as sources for forged reports and inject an unlimited number of bogus reports that fabricate false events "happening" at arbitrary locations in the field. Such false reports may exhaust network energy and bandwidth resources, trigger false alarms and undesired reactions. The authors explain such attacks and that which can be roughly categorised as isolated attacks by each individual compromised node or colluding attacks by a group of collaborating impostors.

Handbook of Research on Advanced Wireless Sensor Network Applications, Protocols, and Architectures-Ray, Niranjan K. 2016-08-01 The implementation of wireless sensor networks has wide-ranging applications for monitoring various physical and environmental settings. However, certain limitations with these technologies must be addressed in order to effectively utilize them. The Handbook of Research on Advanced Wireless Sensor Network Applications, Protocols, and Architectures is a pivotal reference source for the latest research on recent innovations and developments in the field of wireless sensors. Examining the advantages and challenges presented by the application of these networks in various areas, this book is ideally designed for academics, researchers, students, and IT developers.

Open Research Problems in Network Security-Jan Camenisch 2011-02-17 This book constitutes the refereed post-conference proceedings of the IFIP WG 11.4 International Workshop, iNetSec 2010, held in Sofia, Bulgaria, in March 2010. The 14 revised full papers presented together with an invited talk were carefully reviewed and selected during two rounds of refereeing. The papers are organized in topical sections on scheduling,
adversaries, protecting resources, secure processes, and security for clouds.

Cognitive Radio Sensor Networks: Applications, Architectures, and Challenges-Rehmani, Mubashir Husain 2014-06-30 "This book examines how wireless sensor nodes with cognitive radio capabilities can address these network challenges and improve the spectrum utilization, presenting a broader picture on the applications, architecture, challenges, and open research directions in the area of WSN research"--Provided by publisher.

Some Issues in WSN, MANET and Cellular Security- 2007 In this position paper, we address some current limitations and challenges as well as emerging directions in three related areas of secure communication: (1) security in Wireless Sensor Networks - WSNs, (2) security in Mobile Ad Hoc Networks - MANETs, and, (3) security in Cellular Phone Networks.

Secure Wireless Sensor Networks Problems And Solutions

When somebody should go to the ebook stores, search launch by shop, shelf by shelf, it is essentially problematic. This is why we allow the books compilations in this website. It will no question ease you to look guide secure wireless sensor networks problems and solutions as you such as.

By searching the title, publisher, or authors of guide you truly want, you can discover them rapidly. In the house, workplace, or perhaps in your method can be every best place within net connections. If you strive for to download and install the secure wireless sensor networks problems and solutions, it is enormously simple then, before currently we extend the belong to to purchase and make bargains to download and install secure wireless sensor networks problems and solutions for that reason simple!
Secure Wireless Sensor Networks Problems And Solutions


Secure Wireless Sensor Networks Problems And Solutions

Find more pdf books: picture books for children