

Preface

Ad hoc and sensor networks continue to have a growing impact on communication. These cost-effective wireless networks provide location independent computing in environments ranging from military battlefields to in-home patient monitoring systems. However, having real-time connectivity to critical information over an open communication channel requires that the issue of security be addressed. The unconstrained nature of a wireless medium allows for interception, injection, and interference of communication. Moreover, in the absence of centralized infrastructure, nodes must rely on the cooperation of their neighbors to provide data for local processing and to route their processed data. Malfunctions or malicious behavior in ad hoc and sensor networks can cause erroneous results, false alarms, and unaccounted events, crippling the effectiveness of the network. Security solutions for ad hoc and sensor networks are necessary and must be particularly efficient to cope with the constrained resources of these wireless networks.

Scope of Book

Security in Ad hoc and Sensor Networks provides a comprehensive treatment of security concepts from conventional security services to frameworks for managing security. Security issues discussed include (but are not limited to) attacks, malicious node detection, access control, authentication, anomaly detection, privacy and anonymity, key management, location verification, security architectures and protocols, secrecy and integrity, and network resilience and survivability. This complete book provides an excellent reference for students, researchers, and industry practitioners related to these areas.

Authentication and Confidentiality

Part I of *Security in Ad hoc and Sensor Networks* begins with a discussion on two critical services, authentication and confidentiality. Authentication seeks to prove that a device is who it purports to be, while confidentiality aims to preserve the privacy of data from eavesdroppers. Chapter 1 highlights the requirements needed to provide these services explicitly for ad hoc networks. An analysis of the strengths, weaknesses, and overhead are detailed for numerous symmetric, asymmetric, and collaborative authentication solutions. Similarly, the authors also provide analysis for different types of confidentiality schemes that have been proposed in the literature. The confidentiality schemes described go a bit further than just efficiently encrypting payloads to protect privacy of data, but also seek to preserve the secrecy of the participants of the flow. Chapter 1 concludes with a vulnerability assessment of the wireless security protocols 802.1X and 802.11i, the de facto standards for authentication and confidentiality.

The underpinning of many security services, especially authentication and confidentiality, is a secret key. Consequently, mechanisms for establishing, distributing, and revoking keys are critical to the operation of these services. This is particularly challenging for ad hoc and sensor networks because nodes enter/leave the network dynamically and there is no central authority for facilitating these mechanisms. Chapter 2 surveys several key distribution schemes while considering different factors that influence the strategy of a scheme. For instance, implementation of the key distribution scheme may depend on the layer of the protocol stack at which the scheme will operate and on whether the security service is intended for prevention or detection measures. The author of Chapter 2 also evaluates various key distribution schemes based on the storage requirements, network communication bandwidth utilization, and out-of-band communication overhead. Chapter 3 proposes a key pre-distribution framework that exploits the observation that nodes in the same group are usually close to each other after deployment, a characteristic that relaxes the need to discover the correct location of nodes post deployment.

Privacy

Part II, *Privacy*, focuses on the threat to the privacy of information and to the privacy of the participants routing the information. Chapter 4 presents a taxonomy of privacy types and discusses how to measure privacy. The authors then focus on location privacy, discussing issues unique to ad hoc, vehicular, and sensor networks while highlighting the state-of-the-art in each area. Chapter 4 concludes with an analytical methodology for the performance evaluation of location privacy solutions. The model accounts for network performance deterioration and other costs associated with location privacy.

Chapter 5 proposes an anonymizing routing protocol that seeks to preserve topology and location privacy of ad hoc networks. Using bloom filters, the authors enable anonymity of the source and destination nodes and prevent forwarding nodes from inferring other nodes participating in the route. The authors compare the performance of their protocol to the Ad hoc On Demand Distance Vector (AODV) protocol.

The use of wireless sensor networks is emerging in healthcare as a viable solution for continuously and automatically monitoring vital signs in patients. The application of sensor networks to Tele-medicine requires even more restrictive requirements, both legally and technically. Such systems must comply with safeguards (e.g., Health Insurance Portability and Accountability Act (HIPAA)) for protecting the confidentiality and privacy of health information. From a technical point of view, Tele-medicine sensors must have lower complexity and energy consumption and are less tolerant of transmission errors than other sensor networks. Chapter 6 proposes a medical privacy-preserving scheme based on NTRU algorithms. The authors present a hardware implementation and a series of optimizations to achieve the required operation speed and low power dissipation. The authors evaluate the performance of their design for a cardiac sensor network.

Reliability

Part III, *Reliability*, is about the ability of ad hoc and sensor networks to continue operation in the presence of faults that manifest as malfunctions

or malicious attacks. Chapter 7 examines the sources and patterns of faults in sensor networks and identifies metrics for fault tolerance. The authors also discuss current schemes for fault prevention and management. Finally, the authors introduce their own management scheme that focuses on fault detection and recovery for cluster-based sensor networks.

Reliability in the data measurements resulting from phenomena observed in the environment is essential to the accurate functioning of ad hoc and sensor networks. Because the cost of communication is usually more expensive than computation, it is advantageous for a subset of the nodes to aggregate and process data from neighboring nodes locally and to communicate summary data rather than raw data. However, this type of in-network processing increases susceptibility to erroneous results from faulty nodes or malicious attacks. Chapter 8 explains the types of data anomalies that are unique to this context and surveys the state of the art in distributed anomaly detection schemes.

Chapter 9 proposes two techniques for assuring the reliability of data specifically for vehicular ad hoc networks (VANETs). In VANETs, vehicles share traffic information to alert each other of events such as emergencies or traffic congestion. The authors take advantage of the high mobility of vehicles to exploit the low likelihood that vehicles traveling in opposite directions will collude in modifying or forging traffic data. Moreover, a two-directional collusion attack could only occur for the short period of time that the colluding nodes are close to each other. In such a case, subsequent messages would invalidate the malicious data. The authors propose two-directional and time-based schemes to verify the correctness of traffic data in VANETs.

Network Management

Most security research activity for wireless ad hoc and sensor networks has focused on enhancing specific techniques like authentication, encryption, access control and intrusion detection. Little has been done in developing frameworks for managing security services or upgrading the network post deployment. Part IV, *Network Management*, seeks to

integrate powerful lightweight solutions to address these shortcomings, while still adhering to the resource constraints of ad hoc and sensor networks.

Security operations such as encryption/decryption, frame error detection, challenge/response messages, and key exchange messages can be expensive. The ability to dynamically prescribe security operations on the basis of need can extend the life of ad hoc and sensor networks. Chapter 10 discusses the latest technologies for policy-based security management that enable this capability in an energy efficient manner. Radio frequency signals have a limited range, and therefore a wireless attacker can only attack nodes in its vicinity. For that reason, not all nodes are susceptible to the same level of attack at the same time. Propagation behavior is one of the concepts the authors explore in applying security at the right place, time and strength. The authors also conduct an analysis of the energy consumption due to computation and communication of security protocols to illustrate the value of their scheme in security management. Additionally, Chapter 10 presents a case study for a policy-based proactive/reactive security management framework.

Chapter 11 presents a wireless sensor network authorization specification language (WASL) for expressing policies, which can be efficiently communicated throughout the network. WASL distinguishes between the ability to access data and the authorization to do so. For instance, a class of subjects can be authorized to perform a set of actions on a particular data object. This is particularly beneficial for ad hoc and sensor networks where nodes must rely on neighbors for forwarding data, but do not trust the neighbor to operate on the data. The authors demonstrate the implementation of WASL for three different security policy models.

The ability to upgrade existing programs or install new programs post deployment is also essential to the management of ad hoc and sensor networks. A wireless sensor network may need an application patch or new security function added to keep the network operational. It would be impractical to complete this task manually, thus motivating a secure way to do “over-the-air” programming. Chapter 12 surveys recent advancements in dynamic program updates. The authors also propose

two ideas of their own based on the cryptographic hash function and the orthogonality principle.

Many of the protocols used to disseminate program upgrades use version numbers to distinguish new configurations from old ones. Under certain faulty conditions the program updates may not stabilize. The implications of non-stabilizing upgrades could cause a wireless network to carry on forever expending valuable resources. Chapter 13 presents a solution to this problem.